Journal of Theoretical and Applied Information Technology
15th February 2024. Vol.102. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CHOOSING THE RIGHT CHAOTIC MAP FOR IMAGE ENCRYPTION: A DETAILED EXAMINATION

SAAD A. ABDULAMEER
Assistant Lecturer, University of Baghdad, College of Education for Women, Department of Computer Science, Iraq
E-mail: saad@coeduw.uobaghdad.edu.iq

ABSTRACT

This article investigates how an appropriate chaotic map (Logistic, Tent, Henon, Sine ...) should be selected taking into consideration its advantages and disadvantages in regard to a picture encipherment. Does the selection of an appropriate map depend on the image properties? The proposed system shows relevant properties of the image influence in the evaluation process of the selected chaotic map. The first chapter discusses the main principles of chaos theory, its applicability to image encryption including various sorts of chaotic maps and their math. Also this research explores the factors that determine security and efficiency of such a map. Hence the approach presents practical standpoint to the extent that certain chaos maps will become relevant toward implementing image encryption system. This helps them select the best chaotic map for image encryption to ensure secure digital data.

Keywords: *Image Encryption, Chaotic Map, Chaos-based, Image Security, Cipher*

1. INTRODUCTION

1.1. Importance Of Choosing The Right Chaotic Map For Image Encryption

The image encryption is very important for secure storage and transmission of digital images over different digital mediums. As more people require a secure channel of communication and protection of private information, there is a great need to design a strong and resilient image encryption system.

As images possess distinct characteristics (high redundancy (with 50%), pixel correlation of up to 80%, and huge size (with 1GB)), existing encryption methods of AES and DES are inappropriate for image encryption. The application of chaos-based techniques can therefore be seen as a possible strategy for addressing these challenges. Chaotic systems have some unique features like sensitivity to initial conditions, pseudorandom number generation among others, hence suitability for image encryption.

Chaotic maps are one notable characteristic of chaos-based image encryption. Chaos maps are essentially mathematically-based functions characterized by randomness or chaos. These are utilized for blurring and disarray of encoding mechanism. Researchers have investigated using different chaotic maps such as 1D/2D/3D maps for the purpose of image encryption.

Apart from stand-alone chaotic maps researchers have also studied hybrid chaotic maps. They include using multi-chaotic map to improve the security. The mixture of various combinations such as the application of one chaotic map with other ones can increase the overall security for an image encryption algorithm.

In addition, although chaos-based systems have become popular recently for image encryption, some issues should be considered. Some current research utilises one chaos map for encryption and this may need additional security validation. Additionally, some works integrate chaotic maps together with block ciphers or other mixed processes that are not assessed comprehensively for single effectiveness on encoding.

Therefore, a survey on image encryption mentioned that choosing the best chaotic map for securing an image is crucial to achieve better security with good data quality. Chaos-based methods have a number of benefits like dependence on starting conditions, pseudorandom number generation, as well as ergodicity. Yet more studies are required to effectively make a use of chaos theory for developing strong algorithms applicable to various encryption conditions. Chaos-based image encryption systems address several issues,

making it possible to offer a highly effective mechanism for securing digital images in different uses [1], [2], [3], [5], [7], [8].

1.2. Objective of the study

This study has aimed at selecting the most suitable chaotic map to be used in image encryption process. With respect to digital image security various fields have emerged to be of interest. Such areas include multimedia systems, medical communication, and internet communication. It's necessary to construct an effective image encryption algorithm that guarantees high reliability of data storage and transmission process under the conditions of increased level of confidentiality and high image quality. In this regard, existing cryptosystems have demonstrated limited operational efficiency and susceptibility towards the security loopholes especially in regard to image encryption.

For this reason, chaotic systems that exhibit ergodic, non-determinate, and sensitive behavior have developed as an option for encoding. They have some common characteristics with the conditions imposed upon confusion-based and diffusion algorithms like in encryption algorithms. A number of approaches to chaos-based image encryption has been suggested based on both 1D, 2D and 3D chaotic maps. Also, some pieces employ hybrid chaotic maps, which blend the results obtained from different chaotic maps.

A number of studies have proved the efficiency of using hybrid chaotic maps or merging chaos maps with block cipher algorithms in the context of increasing the reliability of image encryption schemes. Still, more evaluation should be conducted to establish an independent efficiency of each approach.

Key space and correlation analysis are some of the parameters that must be considered when selecting the optimal chaotic map for image encryption. Chaotic encryption would reflect the chaotic behavior through rearranging the images pixel values as well as position. This helps mask out the original pixel data in the image, which makes it impossible for the attacker to decipher the message.

Additionally, chaotic encryption uses random keys to guarantee a very strong scrambling of image data during the encrypting as well as deciphering procedures. Thus, this makes the image encryption even more secure.

Although, current works on chaos-based image encryption have shown encouraging results but there remains some gaps. The majority of previous works apply a single chaos bit, combining block ciphers or chaotic maps with insufficient analysis of their security characteristics.

This implies that this paper will explore more on the evaluation and analysis so as to understand each approach of the encryption efficiency. This will help us find out the best chaotic map for the encrypted image which ensures security, reliability, and confidence [1], [2], [3], [5], [7], [8].

2. OVERVIEW OF CHAOS THEORY AND ITS APPLICATION IN IMAGE ENCRYPTION

2.1. Explanation Of Chaos Theory

With an increasing demand for digital image security in the modern, digital landscape, traditional encryption schemes face limitations with regards to image encryption. This problem is overcome through the application of complex dynamical systems referred to as chaotic systems.

Deterministic equations govern apparently random behavior of these systems. Such behavior is perfect for image encryption.

In chaotic systems, the encryption keys or sequence transform the original image to make it unreadable by another person. These are secure because it is quite difficult for another person to know the initial state and thus predict all the steps in advance.

Among other things, there exist chaos maps with dimensions one, two or three (1D, 2D or 3D). Each of them has their ups and downs. Another example is that using one dimensional maps might be easy to implement but may contain limited chaotic range which might also result to an unevenly distributed data. Contrary, 2D & 3D maps have more secureness but consume more computational resources.

Hybrid chaotic maps involving multiple chaotic maps have been suggested as a measure to improve the security of chaos-based encryption systems. This is a good approach as compared to the free standing chaotic encryption system providing more stringent set of security measurement parameters.

For chaotic map selection in image encryption, there are criteria like correlation factors and performance analysis that has to be taken into account. The correlation coefficient is used for defining the extent to which a chaotic map protects an image against having similarity with the original image. The security analysis of an encryption algorithm under different types of attack is included in performance analysis.

As such, chaos theory presents an auspicious means by which to encrypt imaging. Through chaos map, encryption algorithms can ensure confidentiality and better security for high quality encrypted pictures [1], [5], [7], [8], [9], [10], [14], [16].

2.2. Significance Of Applying Chaos Theory In Image Encryption

Chaos theory is very important in digital image processing in ensuring the security and confidentiality of digital data. The term "chaos theory" refers to the science that focuses on the analysis of chaotic systems, the behavior of which is extremely unstable and can only be determined in a probabilistic way even though all parameters describing them are deterministic. Chaos has its inherent randomness and sensitiveness to initial conditions that make it ideal for storing and transmitting digital images.

The chaotic map in image encryption is a dynamical system whose values change with overtime. Map's behavior is very sensitive to the initial set of parameters. This makes it very hard to discover the key and original message unless an attacker knows the correct parameter-values used for encryption or the key itself.

The process of improving the security is achieved by integrating a lot of chaotic maps that yield stronger chaotic maps. It entails integrating maps like Logistic, Tent, Quadratic, Cubic, and Bernoulli maps. The suggested method increases privacy and security by utilizing variable keys derived from computations such as sine square logistic maps.

An appropriate chaotic map must thus be selected for efficient image encryption. It includes choosing the methods of how the correlation values between any two maps affect the picture encryption, as well as the methods of how the choice of two maps influences an end-view of a picture. Lower correlation value shows high quality of encryption.

The results from numerous numerical gray images illustrate how resistant these methods are for encryption as well as decryption of pictures. For performance analysis, they compared other successful methods such as circular mapping, S-boxes, and S-box with Arnold Transform.

Firstly, general characteristics of chaos theory as far as image encryption are concerned. Chaos theory generally helps in image encryption process through providing effective ways of ensuring adequate security, this approach provides improved security levels towards sensitive medical images that are sent via public connections or utilized within telemedicine applications by including numerous chaotic maps and choosing optimal parameters depending on correlation value. [3], [8], [9], [10], [14], [16], [17], [19], [20].

3. DIFFERENT TYPES OF CHAOTIC MAPS AND THEIR MATHEMATICS

3.1. Introduction To Chaotic Maps Used In Image Encryption

The security and privacy of a digital image require that it be encrypted. Since image is big in size and pixels highly correlate, traditional encryption methods do not work here. In particular, chaotic maps demonstrate a chaotic character and are increasingly used in image encryption. There are different types of chaotic maps that are applied differently, including logistic map and quadratic map. The use of several chaotic maps can improve on security and also increase privacy. Nevertheless, certain things cannot be ignored, among them, additional security examination as well as evaluation of encryption feasibility. Chaos-based systems represent a novel approach to image encryption that can be assessed by examining each chaotic map and resolving their weaknesses [1], [2], [3], [4], [9], [10], [11].

3.2. Explanation of various types of chaotic maps

Chaotic maps in image encryption are gaining popularity as they improve security and speed up processing operations. Specifically, there exist some chaotic maps such as tent, logistic, sine, or Henon map with unique mathematical features which can serve as encryption mechanisms. Tent, Logistic, and Sine maps are employed for enhanced security and effective encryption approaches. Additionally, the former maps yield secret/keys that XOR with image pixels leading to changed pixels. Chaotic map in dimension is a new tool that researchers used to solve security problems. It is preferable to use alternate algorithms, based on chaos, compared with the traditional ones. The use of various chaotic maps in its combination may provide higher security levels. Encryption in spatial domain employs changing of pixel values whereas that of transform domain deals on using pixel correlation. The DNA cryptography and LDPC codes would solve the limitations facing this method. Generally, chaotic maps represent a secure and effective approach for performing image encryption; thus researchers can implement more robust algorithms taking into account

characteristics of various maps [3], [4], [8], [9], [11], [12], [13].

3.3. Mathematics behind chaotic maps

Chaotic maps are used in many cases for image encryption because they have features of sensitive to initial conditions and stochastic behavior. Image encryption algorithms have employed a number of types of chaotic maps, such as the Tent, Logistic, or Sine maps. Chaos theory shows that high-dimensional chaos maps are more resistant to attacks than smaller dimensional ones. Studies have demonstrated that using various sets of chaotic maps is a viable technique in image encryption. Chaotic-based cryptography is more powerful than conventional encryption. The choice of a good chaotic map improves the image security and privacy during its transmission. Chaotic maps underpin confidentiality and security in this case. Multidimensional chaos maps, as well a combination of different chaos maps has provided better security for image encryption schemes. Chaos-based cryptography is a viable solution for the limitation of regular techniques [3], [4], [9], [11], [12], [13].

4. FACTORS INFLUENCING THE SECURITY AND EFFICACY OF CHAOTIC MAPS

4.1. Conditions Affecting The Security Of Chaotic Maps In Image Encryption

Several security characteristics of a selected chaotic map for image encryption must be considered when choosing it. The mapping process is essential in any chaotic system used for image encryption. People often use 1D chaotic mapping because of its simplicity, but this approach has security problems and poor chaotic performance. Some of these shortcomings include inadequate sensitivity. One proposed remedy to these hurdles is by providing better traits in two dimensions (Sine adjustment logistic map. This remedy provides a solution that has excellent properties at a relatively cheaper cost.

Thereby, other types of chaotic maps other than the logistic mapping have also been investigated such as affine transformation, gyrator transform, and baker's map. Several factors affect the reliability and safety of chaotic maps. These attributes that demonstrate characteristics of chaos in the chosen map include randomness and sensitivity on initial state value. For better security, chaotic maps of maximum chaos are better.

Another significant determinant that influences the system is the type of an algorithm's structure chosen. This helps to add to the overall robustness of the scheme since techniques such as permutation, diffusion and confusion are combined and integrated together. Another aspect that determines the security level is precision and strength of the selected chaotic map. Chaotic maps may have some errors but they must be robust and strong enough from the security point of view.

This involves considering the encryption speed. Complex chaotic maps may improve security but these maps may slow down encryption/decryption. An important aspect in choosing a chaotic map, especially where encryption of an image is concerned, is striking a balance between security and efficiency.

To summarize, multiple factors influencing the chaos maps security have to be taken into account while selecting best map for image encryption. Chaos property, the map construction methodality, the accuracy as well as robustness of a map and the encryption speed determine the security level and the efficiency of chaotic maps used for images encryption. This analysis should include all these elements, which would aid in selecting a suitable chaotic map for secure and effective cryptographic schemes utilized in image encryptions [1], [8], [14], [16], [17], [19], [20], [23], [24].

4.2. Parameters Influencing The Efficacy Of Chaotic Maps In Image Encryption

While it is an integral part of many image encrypting schemes, it can still be affected by different variables. It is worth mentioning that a particular type of a chaotic map used plays an important role since various maps differ in degree of disorder and randomness. Scientists have investigated lots of chaotic maps including logistic maps and square maps in order to develop sequences which are highly sensitive and unforeseeable.

Security performance of the chaotic map depends on its dimensions. It is however, simplified by one-dimensional (the 1D) chaotic maps which might however be less secure than envisaged. Version 2 of 1D maps demonstrate better performance regarding Lyapunov exponent, complexity, chaos range and sensitivity.

Chaotic maps' behavior and randomness depend greatly on the parametres they use. Carefully selected initial conditions and system parameters promote maximum chaos and unpredictability. The security levels can be improved with encryption

algorithms such as bit-level permutation and wavelet transformation.

Another important criterion for assessing image encryption schemes is computational efficiency. However, there must be minimization on encryption time without compromising security. Using improved key expansion procedures and less iteration cycles to generate keystream reduces encryption speeds.

Security and effectiveness of chaotic maps in images encryption can be assessed through evaluation metrics such as 2D (CC), (IE), (NPCR), (UACI) and etc. These measures inform about the strength of randomness, sturdiness as well as the level of authenticity of the decrypted images.

Finally, the choice and construction of chaos maps, suitable input parameters, cryptography algorithms, compute effectiveness and valid indicators are very important for reliable and speedy images encryption scheme [1], [5], [8], [17], [19], [20], [23], [24], [25].

5. PRAGMATIC VIEW ON THE UTILITY OF CHAOS MAPS FOR IMPLEMENTING IMAGE ENCRYPTION SYSTEMS

5.1. Evaluation Of Different Types Of Chaotic Maps Based On Their Pros And Cons

The efficacy of chaotic maps in various research papers was investigated to assess different types of chaos-based image encryption approaches. Some researchers tried to improve speed and security by combining chaotic encryption and Improved DES. An additional investigation proposed an image encryption scheme built on 2D chaotic map thus added randomness in its dynamic movements. A fast and secure image encryption algorithm based on the chaos system that improves over the previously proposed schemes. The study pointed out that although AES performed highly on security, its encryption running speed was slow compared to chaos based logistic mapping. Security analyses were carried out on an encryption algorithm which included pixel permutations and several chaotic maps that use pixel value encryptions. Various others papers focused on the importance of security issues towards the clinical images and presented innovative encryption techniques. There were surveys comparing benefits of various chaos image encoding algorithms where Arnold's cat map emerged as potentially reliable. There were some studies that suggested new cryptographic techniques that employed chaos and block ciphers. Thus overall, it became evident that the image encryptions using chaos maps provide information about the advantages and disadvantages of chaos maps for image encryption including issues like their security performances, speeds, robustness against attackers, ease of implementation as well as very high security. These findings may be taken as guides for effective development of encryption algorithm based on combination of chaotic maps and other techniques [1], [3], [5], [12], [13], [18].

5.2. Comparative Analysis Of Chaos Maps For Image Encryption

This has made chaotic maps a favourite in image encryption since they create a safe environment that can improve cryptographic schemes for better encryption. There are simple fast and resist attacks. Image encryption has utilized different types of chaotic maps, which are uni-dimensional, multi-dimensional as well as hyper-chaotic maps. Such maps are sensitive to initial conditions, non-predictable, and chaotic like in nature, which make them useful for protecting digital images.

The choice of the most suitable chaotic maps for image encryption depends on the comparative analysis. Performance evaluation of different encryption algorithms is often done using various metrics that include PSNR, correlation, entropy, NPCR, and UACI. When selecting a suitable chaos map for use with PUFs, some factors of consideration include encryption performance, safety levels, computing duration, complexity of implementation, and resistance from attacks.

Many researchers have suggested upgrading existing chaotic maps so that they are more effective. When combined with more efficient ways of encryption like DES or permutations, the use of chaotic maps has proved useful for improving security and expedite. It is important to strike a balance between security and speed while determining the best combination.

In addition, there are numerous approaches for image encryption using chaotic maps and their respective applications. As such, a new image cipher has been proposed using two-dimensional chaotic maps and two-dimensional DWT. New tweak-cube cryptosystems are based on different chaotic maps.

Finally, comparison of chaotic maps is central when it comes to proper image encryption.. The development of newer models of chaotic maps has led to increased security, speed, and robustness against attacks. This calls for future studies targeting perfecting and streamlining these techniques to incorporate in real time encryption over the internet [3], [5], [12], [18], [21], [22].

6. ASSISTING INDIVIDUALS IN SELECTING THE MOST APPROPRIATE CHAOTIC MAP FOR IMAGE ENCRYPTION

6.1. Importance Of Choosing The Right Chaotic Map For Safeguarding Digital Information

However, it is highly imperative to select appropriate chaos maps for protecting digital data. As more and more image encryption techniques emerge in the cyberspace, it becomes necessary to adopt suitable chaotic maps that will ensure safe transmission of digital images over networks.

Over the past few decades, chaotic maps have gathered popularity as a reliable tool in encryption system's ensuring security. Such maps present the high sensitivity to initial conditions, are unpredictable and behave in a way similar to the random ones, making them suitable for cryptographic methods. They have multiple benefits such as easier implementation, high-speed encryption, and strong protection against attackers.

The Arnold map is among the most popular chaotic maps used for imaging encryption. Recently, a work about the image encryption involving Arnold map, DNA sequence operation, and a Mandelbrot set was done. The authors suggested that it would be appropriate to use the Arnold map for the encryption system. Devising a simple and correct map selection strategy was part of the selection process. Using separate encryption for each colour channel in the colour image improved the security.

Moreover, a lot of studies are done with different kinds of chaotic maps (one-dimensional, multidimensional or hyper-chaotic) used in image encryption or scrambling. They have assisted improve the performance of cryptography by using chaos maps alongside other approaches.

The correct selection of a chaotic map is very important, since it is directly related with the safety and efficiency of the image encryption algorithms. In this case, various measures of image quality such as PSNR, correlation, entropy, NCPR, and UACIs are used. These criteria are used in evaluating the efficiency of various chaotic encryption techniques for images.

It's important also to stress that choosing a proper chaotic map should take into account the computation's intricacy and differential attack resilience. However, there has to be a balance between attaining strong security and little encryption time.

Finally, choice of an appropriate chaotic map is crucial for securing images by means of encryption. Chaotic maps have the features of being sensitive to initial conditions and unpredictable to ensure confidentiality and integrity of the transmitted images. Individuals should be keen when choosing an appropriate scheme of image encryption by considering different measures of images quality as well. [3], [5], [6], [12], [15], [18].

6.2. Factors To Consider When Selecting A Chaotic Map For Image Encryption

Therefore, choosing a chaotic map for image encryption is not simple matter and one should take care of several issues before making this choice. The chaotic map has its first factor which comprises of two elements namely sensitivity to initial conditions and chaotic map control parameters. Good encryption demands chaos maps exhibiting extreme sensitivity. Any very small change in these properties will cause large changes in outputs thus making the cryptosystem more secure.

The other significant issue is that the dynamical history of the chaotic map's orbit is also unpredictable. The more erratic the development process, the harder it is for the hackers to crack the encrypted image. This randomness that characterizes the whole process helps to make it difficult for hackers, thereby enhancing the security level of the whole scheme.

Another factor includes the use of simple hard- and software components. Hardware and software chaotic maps allow faster encryption of large images like those captured by CCTV/Cameras or other real-time applications.

In addition, one has to determine whether the selected chaotic map gives sufficient encryption amount. Faster processing time is achieved for an increased encryption rate at no compromise of the overall security. It is this characteristic which contributes to the effectiveness of the encryption algorithm itself.

Also, it is important to consider the balance and avalanche characteristics of a chaotic map. The strength of confusion and diffusion of chaotic based encryption algorithm is dependent on these attributes. The mixing transformation function used for such systems should be very sensitive – any deviation of any of the input parameters has to lead to significant changes of the output variables.

However, one ought to also assess any particular characteristics or constraints of various image kinds or varieties. The image encryption algorithm could thus be designed to handle compressed and

uncompressed data sets or be compliant with compressed data formats such as GIFs or JPEGS or be scalable. Having knowledge of these requirements enables one to determine if there is any chaotic map that suits specific image types and forms.

Lastly, I should mention any extra features or upgrades that some chaos maps provide. For instance, some maps can use different types of encryption methods which are multi-levels, or make computations simpler for realistic purposes.

Thus, these aspects should be considered before deciding on the best chaotic map suitable for an image encryption process. These factors will help to enhance the safety, reliability and suitability for different kinds of pictures as well as software programs [3], [4], [5], [12], [15], [18], [21], [22], [23].

7. THE PROPOSED SYSTEM

This pseudocode outlines a process for choosing the right chaotic map based on certain criteria. The choose_chaotic_map function iterates through available chaotic maps, evaluates each map's suitability using the evaluate_chaotic_map function, and selects the one with the highest score. The analyze_image function is responsible for extracting relevant properties from the image that can be used in the evaluation process.

```
function choose_chaotic_map(image_properties):
    available_chaotic_maps =
    get_available_chaotic_maps()
    // Criteria for choosing the right chaotic map
    selected_map = null
    best_map_score = 0
    for chaotic_map in available_chaotic_maps:
        map_score =
        evaluate_chaotic_map(chaotic_map,
        image_properties)
        if map_score > best_map_score:
            best_map_score = map_score
            selected_map = chaotic_map
    return selected_map

function get_available_chaotic_maps():
    // Return a list of available chaotic maps

function evaluate_chaotic_map(chaotic_map,
image_properties):
    // Evaluate the chaotic map based on image
    properties
    // Consider factors like sensitivity to initial
    conditions, key space, statistical properties, etc.
    return map_score

function load_image(image_path):
    // Load the image from the specified path

function normalize_image(image):
    // Normalize pixel values to [0, 1]

function implement_chaotic_map(map_type,
parameters):
    if map_type == "logistic_map":
        return initialize_logistic_map(parameters)
    else if map_type == "henon_map":
        return initialize_henon_map(parameters)
    else if map_type == "lorenz_system":
        return initialize_lorenz_system(parameters)
    else:
        raise UnsupportedChaoticMapException
            ("Unsupported chaotic map type")

function initialize_logistic_map(parameters):
    seed = parameters.seed
    r_value = parameters.r_value
    iterations = parameters.iterations
    chaotic_sequence =
    generate_logistic_map_sequence
    (seed, r_value, iterations)
    return chaotic_sequence

function initialize_henon_map(parameters):
    // Similar structure as initialize_logistic_map,
     tailored for Henon map

function initialize_lorenz_system(parameters):
    // Similar structure as initialize_logistic_map,
    tailored for Lorenz system

function generate_logistic_map_sequence(seed,
r_value, iterations):
    // Generate a chaotic sequence using the logistic
    map

function bitwise_xor(array1, array2):
    // Perform bitwise XOR operation between
    corresponding elements of two arrays

function create_image_from_array(array):
    // Create an image from the array

function save_image(image, path):
    // Save the image to the specified path

function encrypt_image(image_path,
chaotic_map_type, chaotic_map_params):
    original_image = load_image(image_path)
```

```
    original_array =
normalize_image(original_image)
    chaotic_sequence = implement_chaotic_map
            (chaotic_map_type, chaotic_map_params)
    encrypted_array = bitwise_xor(original_array,
                    chaotic_sequence)
    encrypted_image = create_image_from_array
                        (encrypted_array)
    save_image(encrypted_image,
                'encrypted_image.png')

function analyze_image(image_path):
    // Analyze the image and extract relevant
      properties
    // Properties may include size, color distribution,
    entropy, etc.

function main():
    image_path = 'path_to_your_image.jpg'
    image_properties = analyze_image(image_path)
    selected_chaotic_map = choose_chaotic_map
                            (image_properties)
    encrypt_image(image_path,
        selected_chaotic_map, { 'seed': 0.5, 'r_value':
        3.8, 'iterations': 1000 })
```

8. CONCLUSIONS

Therefore, chaotic maps have now been used as a viable technique of encrypting images, which is the key to ensure secure transmission of digital multimedia communications over internet. Several of them come with various algorithms, which they designed to augment the efficiency of the encryption and safety of image encryption systems.

These approaches include compound chaotic maps and random cyclic shift. HLITC is a hybrid chaotic system that was designed by connecting logistic, ICMIC, tent, and Chebyshev maps, which showed higher chaotic performance than other chaotic systems. The improved HLITC random number generator chaotic system then leads to the proposed image encryption algorithm using two circular shifts. HLITC generates key sequences for scrambled and diffused images, based on a spiral transform dictated by a chaotic sequence and XOR operation controlled by a chaos map.

There has been a lot of experimentation towards validating the above encryption system. The statistical analysis is one of the experiments while other ones are key sensitivity analysis, and keyspace analysis. It is evident that the presented design of a new encryption scheme is robust in terms of brute force attacks, statistical attacks and differential attacks. This encryption algorithm is better than several of them that are used today for chaotic image encryption.

Such systems as RSA, AES, DES, and IDEA can hardly be used for image encryption because of its distinctive traits like large amount of packed data, high redundancy level, and a lot of correlation between neighbouring pixels. The chaotic maps possess remarkable features which fulfil fundamental descriptive of an encryption technique like sensitivity concerning onset data and parameters. Further, they exhibit fast decay on auto correlation function with no recurrence as well as randomness, infinity on key room and very much complicity.

Chaotic maps are diverse, for example, they can be (1D) or (HD). 1D chaotic maps have been shown to be relatively weak against phase space reconstruction based attacks; HD chaotic system provides much better security but comes at the expense of both costly implementation and slow processing speeds (encryption and decryption). Hence, an accurate strategy entails incorporating positive characteristics of both types of chaos-based encryption schemes in designing encryption algorithms.

Recently, several supplementary ways including MD5 algorithm, piecewise chaotic maps, DNA rule and 3D Lorenz chaotic systems have been mixed with chaos-based image encryption methods in order to enhance the protection capability. Nonetheless, these additional tactics might hamper the speed of encryption.

In general, studies on encrypted image via chaotic maps have produced considerable advancements to enhance secure encrypted image procedures. This is evidenced by relatively strong immunity against attacks and low complexity of computations of the suggested algorithms. Nevertheless, such research direction still provides an opportunity for additional searching and upgrading. Therefore, future works can be in creating more potent encryption techniques resistant to modern attacks and increasing encryption/decryption speed that is secure as well [7], [18], [21], [24], [26].

REFERENCES:

[1] Chaudhary, N., Shahi, T. B., & Neupane, A. (2022). Secure image encryption using chaotic, hybrid chaotic and block cipher approach. Journal of Imaging, 8(6), 167. https://doi.org/10.3390/jimaging8060167

[2] G, V., & M, R. (2021). A survey on image encryption using Chaos-based techniques. International Journal of Advanced Computer Science and Applications, 12(1). https://doi.org/10.14569/ijacsa.2021.0120145

[3] Rehman, M. U., Shafique, A., Khalid, S., & Hussain, I. (2021). Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps. IEEE Access, 9, 52277–52291. https://doi.org/10.1109/access.2021.3069591

[4] Sudeep, N. B., Ravindra, S. (2023) Design and Development of Multidimensional Chaotic Maps with Genetic Operator. I. J. Mathematical Sciences and Computing. MECS Press (http://www.mecs-press.org/) https://doi.org/10.5815/ijmsc.2023.03.02

[5] Khairullah, M. K., Alkahtani, A. A., Bin Baharuddin, M. Z., & Al-Jubari, A. M. (2021). Designing 1D chaotic maps for fast chaotic image encryption. Electronics, 10(17), 2116. https://doi.org/10.3390/electronics10172116

[6] Jithin, K. C., & Sankar, S. (2020). Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. Journal of Information Security and Applications, 50, 102428. https://doi.org/10.1016/j.jisa.2019.102428

[7] Rashmi, P., & Supriya, M. C. (2021). Optimized chaotic encrypted image based on continuous raster scan method. Global Transitions Proceedings, 2(2), 589–593. https://doi.org/10.1016/j.gltp.2021.08.055

[8] Jain, K., Aji, A., & Krishnan, P. (2021). Medical Image Encryption Scheme using multiple chaotic maps. Pattern Recognition Letters, 152, 356–364. https://doi.org/10.1016/j.patrec.2021.10.033

[9] Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (2021). A new algorithm for Digital Image Encryption based on Chaos Theory. Entropy, 23(3), 341. https://doi.org/10.3390/e23030341

[10] Yousif, B., Khalifa, F., Makram, A., & Takieldeen, A. (2020). A novel image encryption/decryption scheme based on integrating multiple chaotic maps. AIP Advances, 10(7). https://doi.org/10.1063/5.0009225

[11] Lin CY, Wu JL. Cryptanalysis and Improvement of a Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion. Entropy (Basel). 2020 May 24;22(5):589. PMID: 33286361; PMCID: PMC7517126. https://doi.org/10.3390/e22050589

[12] Kumar, N., Wadhwa, D., Tomer, D., & Vijayalakshmi, S. (n.d.). Review on different chaotic based image encryption techniques. Ripublication.com. Retrieved October 25, 2023, from https://www.ripublication.com/irph/ijict_spl/ijictv4n2spl_14.pdf

[13] Zolfaghari, B., & Koshiba, T. (2022). Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap. Applied System Innovation, 5(3), 57. https://doi.org/10.3390/asi5030057

[14] Li, R., Liu, Q., & Liu, L. (2019). Novel image encryption algorithm based on improved logistic map. IET Image Processing, 13(1), 125–134. https://doi.org/10.1049/iet-ipr.2018.5900

[15] Li, C., Luo, G., Qin, K., & Li, C. (n.d.). Chaotic image encryption schemes: A review. Atlantis-press.com. Retrieved October 25, 2023, from https://www.atlantis-press.com/article/25875804.pdf

[16] (N.d.). Europepmc.org. Retrieved October 25, 2023, from https://europepmc.org/article/pmc/4131117

[17] Kanwal, S., Inam, S., Hajjej, F., Cheikhrouhou, O., Nawaz, Z., Waqar, A., & Khan, M. (2022). A new image encryption technique based on sine map, chaotic tent map, and circulant matrices. Security and Communication Networks, 2022, 1–17. https://doi.org/10.1155/2022/4152683

[18] (N.d.). Researchgate.net. Retrieved October 25, 2023, from https://www.researchgate.net/publication/222697807_An_image_encryption_approach_based_on_chaotic_maps

[19] Zhu, S., & Zhu, C. (2021). Security analysis and improvement of an image encryption cryptosystem based on bit plane extraction and multi chaos. Entropy (Basel, Switzerland), 23(5), 505. https://doi.org/10.3390/e23050505

[20] Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. Entropy (Basel, Switzerland), 23(3), 341. https://doi.org/10.3390/e23030341

[21] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and

spatiotemporal domains. International Journal of Information Security, 21(4), 917–935. https://doi.org/10.1007/s10207-022-00588-5

[22] Mfungo, D. E., Fu, X., Xian, Y., & Wang, X. (2023). A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information. Applied Sciences (Basel, Switzerland), 13(12), 7113. https://doi.org/10.3390/app13127113

[23] Wikipedia contributors. (2023, October 14). Chaotic cryptology. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Chaotic_cryptology&oldid=1180126434

[24] Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., & Miao, S. (2018). Image block encryption algorithm based on chaotic maps. IET Signal Processing, 12(1), 22–30. https://doi.org/10.1049/iet-spr.2016.0584

[25] Zolfaghari, B., & Koshiba, T. (2022, July 21). Share an online entry "chaotic image encryption." Encyclopedia.Pub; Behrouz Zolfaghari. https://encyclopedia.pub/entry/25377

[26] Alawida, M. (2023). A novel chaos-based permutation for image encryption. Journal of King Saud University - Computer and Information Sciences, 35(6), 101595. https://doi.org/10.1016/j.jksuci.2023.101595