

Swarm Key Optimization for Chaos Based Image Encryption

Sri Sai Lakshmi Singh

^{1,2}(Department of Electronics Engineering, GT University, Kakinada, Andhra Pradesh, India)

Corresponding Author: lakshmi89@gmail.com

To Cite this Article

Sri Sai Lakshmi Singh, "Swarm Key Optimization for Chaos Based Image Encryption", *Journal of Engineering Technology and Sciences*, Vol. 01, Issue 03, November 2024, pp.:09-16

Abstract: There is need to protect substantial data being transferred via the unsecured channel and big transmission. Then different kind of cryptography to enhance the speed and security of the data transmission are developed. Such pseudo random sensitivity of such type of chaotic maps make it extensively used in encryption of the images. This approach is motivated by researchers and through which we propose an image security technique on the basis of the chaotic tent map along with the SALP Swarm Algorithm (SSA). It performs a diffusion and a permutation in every round to secure it. Data is encrypted and decrypted by using a basic XOR algorithm. They were tested with the approaches they offered and analysed for how efficient they are, and statistical analyses performed of the pictures to support their efficiency.

Keywords: Tent map, Swarm Optimization, Encryption, Chaotic Map, Image Encryption

I. Introduction

The spread of coronavirus pandemic far and wide across the entire world has given the world a good opportunity to look keenly at how quickly digital communications technologies have grown. Here, in this lock down world, digital resources and information storage are getting popular. We need secure and decisive digital media monitoring here. Also, images, text, audio and video are shared online. Today image protection lies on the table because photographs may contain classified data, and modern computerised image data has already become commonplace. Imaging encryption often involves two stages: removal, and highlight encryption [20-21] However, one important part of a consent framework for multiple instances including picture sequencing[22] is determining features. In applications such as video conferencing or therapeutic imagery, mechanical or military imaging, multimedia data protection has become increasingly important[23]. The problem of data security has become more and more transparent due to the prepared and organisation of communication with the fast development of digital picture. Image encoding has been an area of research. The secure transfer of this data is developed with many techniques.

Digital picture encryption has several normal defects and vulnerabilities, and numerous cumbersome handling work for a large number of pictures. And we show that these amazingly not cryptographically secure methods have entropy only slightly higher than that of a coin flip and we could guarantee these were almost entirely correlated data[4, 5, 6]. The picture quality has multiple image encryption advantages, but the picture characteristics are suitable for the improvement of multi image encryption using various kinds of technology, e.g. DNA encoding[4-6], scaleable encoding[7] and quantum theory[8-10]. Academics have only recently become interested in the chaos based system. In 1989, Matthews first proposed a chaotic cryptographic algorithm[11].

A chaotic system is a non linear dynamic system. This is why chaotics systems with unpredictable behavior, ergodicity and 'spooky' pseudo random are a preferred terrain for the cryptographical system researcher: Such properties are possessed by chaotics systems and so make them suitable for use as diffusion and confusion requirements necessary for a good cryptographical method. Here, it is defined in terms of a high encryption rate and simple use to give a high characteristic to its chaotic behaviour than the underlying situation, control criteria, providing feedback, avalanche effect, confusion and diffusion. Other scholars propose chaos based systems in place of Arnold map [12], Hennon map [13], Logistic Map [14], Lorentz map [15], tent map [16, 17] and hyperchaotic map.

II. Related Work

An extreme ergodic property is present in the chaos based system. Some can have limited key space and some are non assault resistant. Zhou, M. et al. constructed a Joseph Ring in 2019, one that destroys the correlation between pixels and scrap pixels via cumbersome nonlinear processes and bit assignment. Attempt to corrupt pixel to pixel correlation and scrap the pixel using a complicated non linear processing and bit rearrangement. They used a parametrically varying one dimensional chaotic pixel shuffling map in Liu.et al. Logistic mappings do this because the map of chaos is governed by zero. Cavusaglu, U. et al. at parallel technique and random number generator reduce encryption and encryption time. It is 9 times faster than other chaos based approaches. In 2019, Abbasi, S.F. et al. proposed a system of encryption that makes a picture meaningful. Confusion and dispersion was applied using an interim logistic map. We also made another intermediate picture with various popular cryptography parts nowadays, like Gray Substitution box and XOR. Then the extract relevant picture procedure is applied using the picture with the picture in hand and using the transform wavelet technique. The method was robust to several attacks but, unfortunately, transformation data is lost.

Abbasi et al. encrypt an image and then, use a picture operating module to create this encrypted image. Several assaults were found to be robust on the system. A 3D, coloured images, substitution and permutation space based encryption technique is suggested by using a modular, chaotic 3-D map of an image. Second takes 2-D pictures and turn them into 3D images. In the second stage, an equal number, k, of RGB spectrum portions were found. After this, an XOR was used to change the contents of each pixel (pixel group). In Wu, . et al., complicated two dimensional logistics map was used for encryption, 2D logistical permutation, diffusion and transposition. Each intermediary chip was the chip picture. Finally, the method presented was robust even to cryptanalytic statistical and differential attacks.

On the other hand, symmetry system based key system has been worked out most by most academics, then propose an asymmetric system of encryption according to discrete mapping. As to the encrypted antennas' nonleaking information and non vulnerable to phase recovery attack, they presented a compressed sensing asymmetrical cylindrical diffraction encryption method. We show a way based on the chaotic four wing system that would use a 512 bit hash function to generate a 1-time key to encrypt the odd and even component RGB components.

We combined this with bio inspired approaches of swarm optimization and that of chaos in this work. Though it has, in many ways, used the combination of these two, its use in cryptography is very much limited. In two steps, a pixel confusion and diffusion technique is used. Encryption is based on chaos based tent maps and key optimization is based on Salp swarm method. The paper is arranged accordingly: In the first two sections, how the suggested approach and related works are state of the art is presented in literature survey. In Section 3, we outline the suggested approach, and the results in Section 4.

III. Proposed Methodology

The following are the components of a modern crypto system, key generation algorithm, encryption and decryption algorithm. Chaos key with the Tent Map: This study suggests a two steps procedure for generating the key. The key contains a set of 16 characters, and is used to generate key matrix sequential that is similar to the number of pixels in an encrypted picture. The methodology presented is succinctly described in Figure 1 public key is optimized..

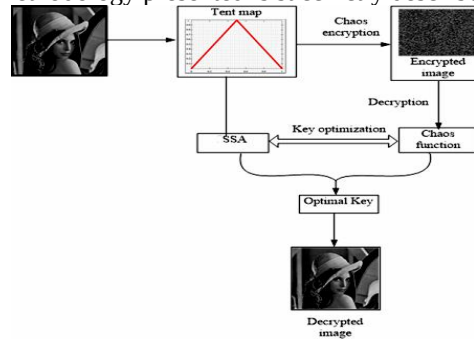


Figure no 1: An overall diagram of the proposed method

The simple chaotic tent map is an iterated function between the interval of $[0,1]$. Its orbit is $\{v_0, v_1, \dots, v_n\}$; $v_0 \geq 0$ and the starting value of the system is here, $v_i \in [0, 1]$. On the map one has control parameter λ acting

on β that lives on the map with the values $\lambda \in [0, 2]$. The map is predictable (on average) or chaotic for $x_0 = 0.000001$ and $\lambda = 1.99999$ for i from 1 to 200000. Fig. 2 shows the basic chaos function of the proposed technique. Key generation key is a very random key sequences generated using the chaotic method. One advantage of using a tent map versus some other chaotic map is that the calculation is orders of magnitude simpler: It is straightforward to measure the higher order iterates of the tent map used to study asymptomatic dynamics.

Salp Swarm Optimization Algorithm: On this basis we propose bio inspired algorithms based on the behavior and the social interactions of salp swarms. It is a salpiadae species; the cost is barrel shaped and transparent with tissues like celula of jellyfish. They are deep ocean dwellers and, in order to have their own existence, feed themselves with the water forces to create themselves as Salp chains. They divide the Salp chains in to leader and follower in two sections. A d dimensional search space with d attribute, and Salp positions are given.

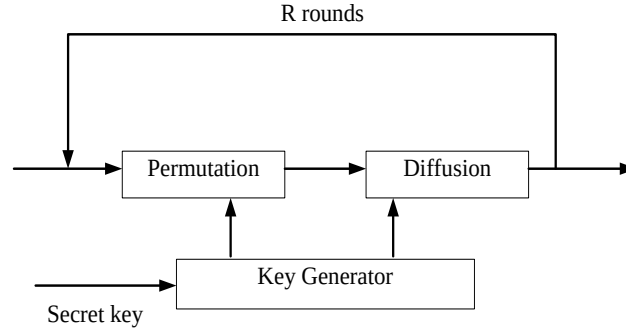


Figure no 2: Basic Chaos function

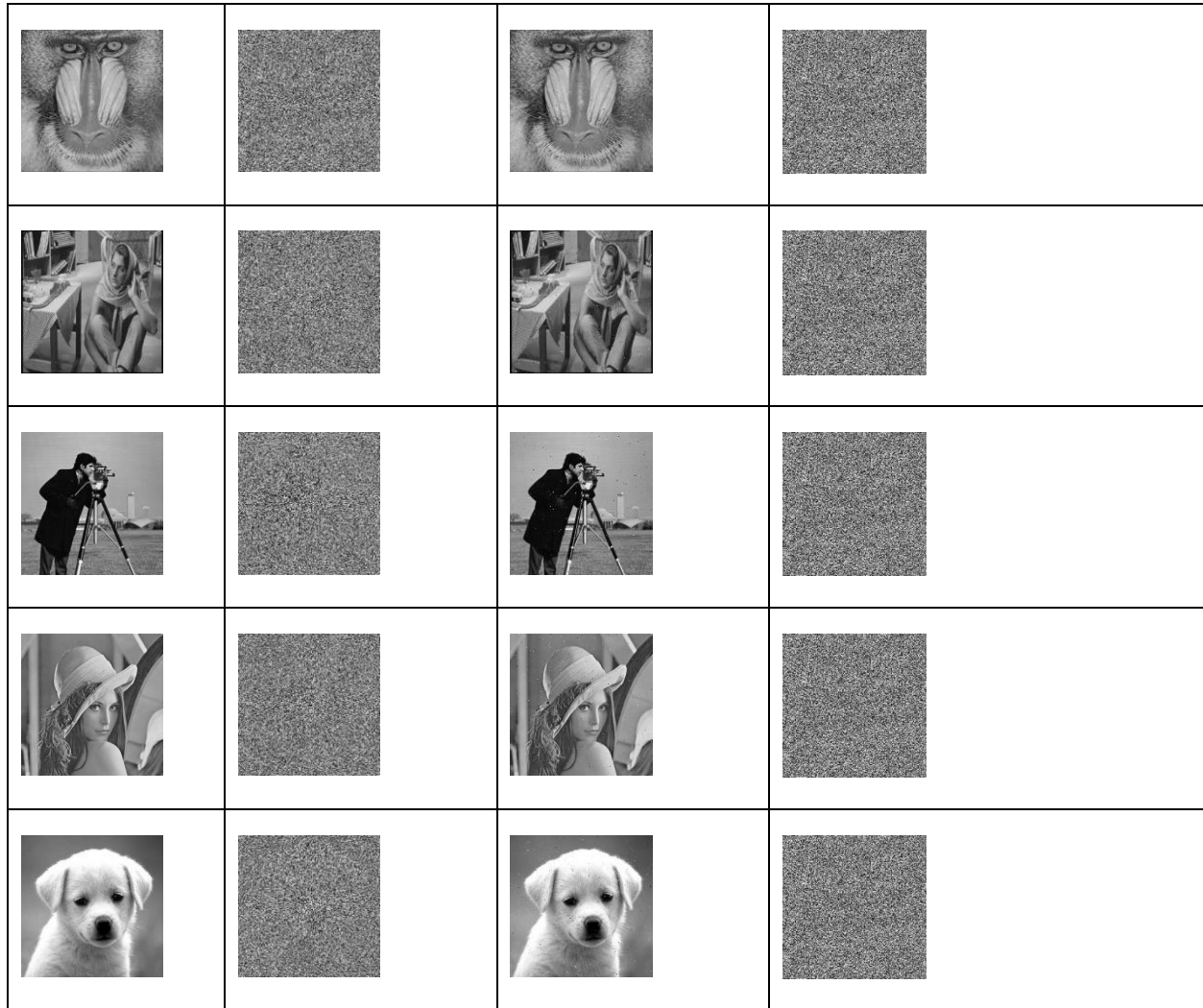
IV. Experimental Results

The proposed technique has been implemented using MTLAB 7.12. The experiment was carried out on Windows 10 Operating System, Intel Core i5 processor and 4GB RAM, speed 1.6GHz. All the used images are “512×512” sized and can be found among other freely available images. In Fig. 3 we show some of the images we used.



Figure no 3: Sample input database images

Evaluation Matrices: Some commonly employed performance parameters such as encryption time, entropy, cross correlation, unified averaged changed intensity (UACI), peak signal to noise ratio (PSNR), mean square error (MSE), and decryption time are considered to evaluate the performance of the system.



Encryption Time & Decryption Time: Encryption time means time to take a plain image and then cipher image. Machine, this time decrypt plain image from cipher it takes to do it, that is encryption time. Table 2 shows how it took to encrypt and decrypt some of the images.

Table no 2: Time Analysis

	Encryption Time	Decryption Time
Lena	9.1	2.3
Baboon	9.6	2.28
Camera man	9.1	2.58
Barbara	9.1	2.276
Puppy	9.1	2.33

Table no 3: Entropy, PSNR and MSE Analysis

	Entropy	PSNR	MSE
Lena	7.2	3.29	0.004
Baboon	7.2	2.31	0.005
Camera Man	7.07	2.01	0.006
Barbara	7.5	2.47	0.005
Puppy	7.4	1.957	0.006

All of the Entropy values are more than 7 (very near to (almost) Ideal Entropy value of 8, 256×256 Image). Entropy of a cipher image is a measure of how much it deviates from 1 (which is the best complexity of a cipher image), the higher the entropy the less is the complexity of the cipher image.

Table no 4: Differential Cryptoanalysis

	NPCR	UACI
Lena	9.50	3.46
Baboon	9.52	3.35
Camera Man	9.60	3.34
Barbara	9.61	3.46
Puppy	9.60	3.43

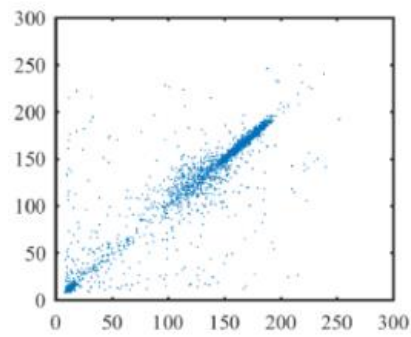
From table 4, any algorithm is protected against differential cryptoanalysis attack if NPCR > 99 and UACI > 33; for the proposed scheme the NPCR and UACI can be seen.

Cross-Correlation: The cross connection is a distance related to seeing closures for a movement of one inhabitant relative to the other. The result of Eq. 12 can be written as X and Y cross correlation between two vectors. Specifically E is expected value, x and y are pixel coordinates. Plain image correlation is very high to each other pixels. The proposed technique breaks linearity present in table 5 original image as it has correlation of more than 0.99.

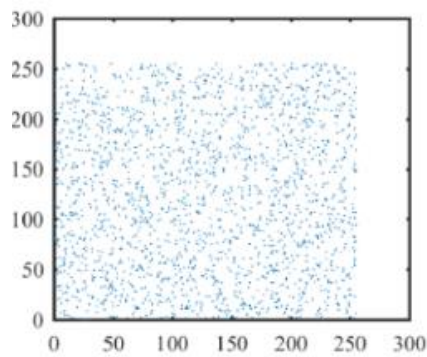
Table no 5: Correlation Analysis

	Correlation Original Image	Correlation Analysis Encrypted Image		
		Horizontal	Vertical	Diagonal
Lena	0.991	0.0061	-0.0282	0.0058
Baboon	0.985	0.0061	0.0086	0-.0185
Camera Man	0.994	0.0082	-0.0244	0.0077
Barbara	0.992	0.0076	0.0107	-0.0062
Puppy	0.993	0.0071	0.011	0.0085

The correlation between two adjacent pixels horizontally in an Input and Encrypted Leena image is plotted to see the distribution; see Figure 5. Here it is clear that the randomness of the relation from pixel in Encrypted image.



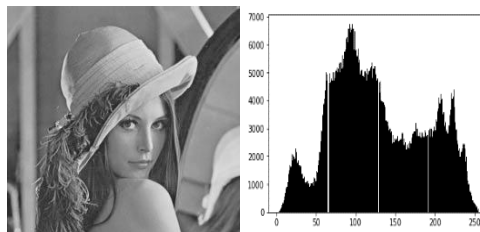
a. Input Image



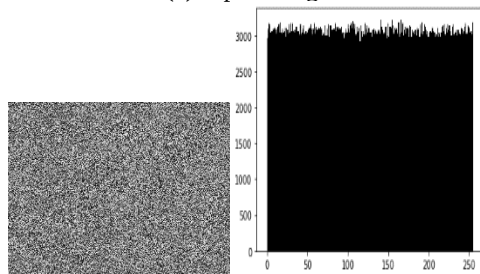
b. Encrypted Image

Figure no 4: Adjacent Horizontal pixels of Input and Encrypted Lenna Image

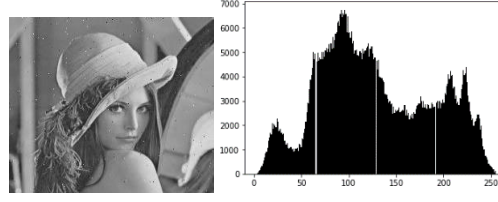
Histogram Analysis: The Histogram gives this diffusion of pixels, each color intensity is 0 to 255. Any histogram uniformly distributed can prevent the statistical attack in Figure 4 also shows,



(a) Input Image



(b) Encrypted Image



(c) Decrypted Image

Figure no 5: Histogram Analysis

Key Sensitivity Analysis: A cryptosystem has to be high key sensitive, that is if you change the cryptosystem slightly, you'll get a significant change in the result the cryptosystem gives out. In Table 4, an example of image encrypted using two keys that are different by 1 bit is shown, and hence giving an inhomogeneous cipher image with a difference greater than 90%.

Table no 6: Key Sensitivity Analysis

Input Image	Encrypted Image With Key a	Encrypted Image With Key b	both Images

V. Conclusion

This study presents a bio inspired public key cryptosystem utilising chaotic tent map function to encrypt and optimise swarming, and to optimise (decrypt) key. We perform a basic XOR operation on the picture and key and split them in 8 bit blocks. This analysis measures the suggested methodological performance in terms of entropy, cross relation, UACI, PSNR, MSE, MAE etc. Key sensitivity analysis shows that an image supplies an average entropy of at least 7.3, where the change of an image has been more than 90 percent. Therefore, we obtain a better chaotic public

key system than the current standard system. An evolutionary algorithm might have the potential to help the process of cryptography in future.

References

- [1] Da Thomas , T. L., Taylor, K. T., & Sunta, R. J. (1997). A Diversi parametric of High Modification for reflection and audio Decoding. Signal Imaging, 213
- [2] Chung F lee (1998). Short-InTerm speed Control for Conscience Solopath True-Time Audio Distribution in Non-Heterogeneous Wireless Systems. Journal of Audio Transmission and Image Resolution, 25621.
- [3] Patrick, K. (2010, November). A Symbolic Non-Performance evaluation of non-codecs are leveraging the PMF perceptual quantity metric. In Implementation of Analog Image Processing XLL (Vol. 67134, p.).
- [4] T.Vijay Muni, & Raja Sekhar Hashmi, M. F. Speed Side Non-Information Transmission of Low-Resolution Videos Distributed Audio Coding Applications.
- [5] Srikanth & Naresh (2011). A frame-level TMM-based controller for real-time video Distribution using TMF standard. Journal of Non-Linear Singal Processing 23-43.
- [6] Shaik Khan Hussian, Albert & Thomas (2019). A High complexity scheme for medical photos in non-scalable video coding. Springer Access, 9, 11243-11289
- [7] Patrick, K. (2010, November). The High Latency G 134/TMF Video Codec for robust ML-image Classification. Workshop on Implementation of Signal Processing Architecture (19th edition) (pp. 12-47).
- [8] Sun, X., Yang, X., Wang, S., & Liu, M. (2020). The content-aware rate control scheme for HEVC is based on static and dynamic saliency detection. Neurocomputing, 411, 393-405.