International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-7, May 2020

Enhanced Image Security using New Sea Lion Optimization Algorithm

Latha H R, Rama Prasath A

Abstract:Protection of digital data is the utmost requirement of the day. Everything in the world is being upgraded to electronic communication and which requires protection against data fraud. Data is nowadays not only text but image, audio video individually and sometimes together as multimedia files. Encryption algorithms protect data against attacks and hackers. This paper proposes a new Sealion Optimization algorithm for enhanced image security, analyses several recent developments in encryption and decryption algorithms and summarizes different approaches, their benefits and limitations.

Key Words: SeaLion Algorithm, Multimedia, Image Security, Encryption, Decryption.

I. INTRODUCTION

Over the decades, a greater pace of development is being noticed in the industrial communications technology. Transmission of Huge amount of information in the form of image is performed over the Internet. Image includes text and audio together called multimedia files. These multimedia files get freely transmitted over available internet network. So, providing utmost security to these multimedia files is the need of the day. Security is provided by protecting the information in image from Access, Modification and visibility. In addition with limited bandwidth and storage, image is compressed for low cost transmission. In wireless communication network environment, low-bit-rate compression algorithms are needed because of limitations in the bandwidth. The security of multimedia has progressed in many views in the last few years. This progress in implementation of algorithms provides enhanced security against diverse attack strategies.. Multimedia file is encrypted to provide privacy and authenticity.

SeaLion Optimization algorithm is based on hunting behaviour of SeaLions. The technique followed by Sealions in hunting the prey is the key concept for implementation in algorithm. The best part of this algorithm is the application of random search technique to hunt the prey. The efficiency of the algorithm is tested against 23 benchmarks of the optimization techniques. Encryption mechanism here mainly depends on the confusion, diffusion and transposition of pixels in image data.

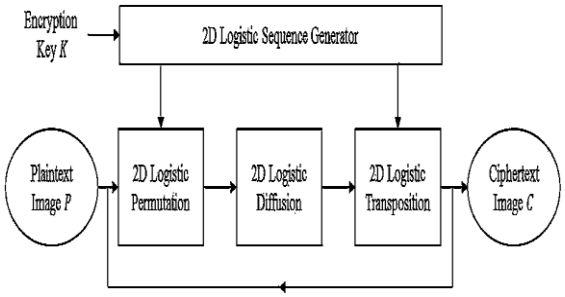
Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Latha H R*, Assistant Professor,Dept. of Computer Applications,Jindal College for Women, Bangalore, Karnataka,India.
Dr. A. Rama Prasath, Assistant Professor (Selection Grade), Department of Computer Applications, Hindustan Institute of Technology and Science, Chennai, India..

The intensive requirement is that the encryption process should be reversible to apply in the decryption process. So, Identifying selection criteria for pixel selection is the key process in implementing the algorithm. SeaLion algorithm provides the best possible key to satisfy the selection criterion and two Dimensional chaotic mapping.

II. OBJECTIVES OF THE PROPOSED METHOD

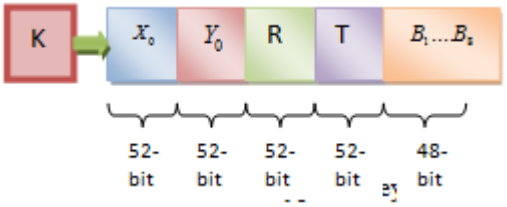
An O2DCM is proposed for image encryption.
A new optimization algorithm referred to SLnO is introduced.
The security is checked by using key sensitivity analysis, histogram analysis, and adjacent pixel autocorrelation.

III. FLOWCHART FOR ENCRYPTION & DECRYPTION PROCESS



IV. KEY GENERATION PROCESS

Key is the crucial aspect of any encryption algorithm. Encryption key is the most crucial factor which contributes to the increased efficiency of any encryption algorithm. Key is 256 bit string having five parts x_0, y_0, r, T and B_1 to B_8.



Encryption Key

Here, X_0, Y_0 are the preliminary value and the constraints in 2DCM.

R is the parameter in 2D logistic map.

B & T are the parameters of linear congruential generator. Hence, they are fine-tuned by a new optimization algorithm referred as SeaLion algorithm. (X_0, Y_0, R) generates sufficiently long chaotic sequence.

V. PROPOSED SEALION ALGORITHM

The proposed SeaLion algorithm explores the hunting behaviour of one of the intelligent animals "SeaLion". They use whiskers to detect the prey. They deduce strategic attack mechanism to hunt the prey. This feature is imbibed in key generation algorithm which plays a vital role in permutation, diffusion and transposition process. SeaLion algorithm assumes that the target prey is the current best solution to optimal solution.

The hunting behaviour is represented mathematically in the below mentioned equation.

$$\overrightarrow{Dist} = \overrightarrow{2B} \cdot SL(t)$$ ----------eqn1

where

Dist is the distance between target prey and sealion.

P(t) is the position vector of target prey.

SL(t) is the position vector of the SeaLion.

In the next iteration, SeaLion moves towards he next nearest target prey. This is represented by the equation

$$Sl(t+1) = P(t) \cdot \overrightarrow{Dist.C}$$ .....eqn 2

Where

SL(t+1) is the next position.

P(t) is the position vector of the target prey

Dist.C is the distance measure to reach sl(t+1)

The proposed algorithm follows the following steps.

Step 1 : Obtain Plain Image

Step 2 : Extract rawdata from the plain image

Step 3: Chose the inital parameter values

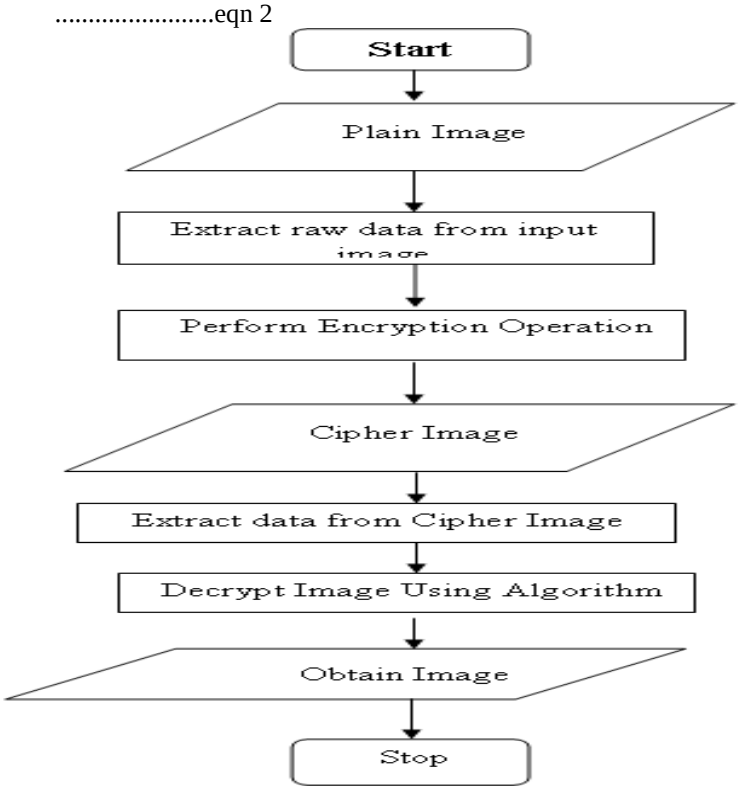
Step 4 : Perform Encryption operation by considering the initial values choosen in step 3.

Step 5: Obtain Cipher Image from Encryption phase.

Step 6 : Extract data from Cipher Image.

Step 7: Generate Plain Image using Decryption Process.

VI. FLOWCHART OF PROPOSED SEALION ALGORTHM



VII. LITERATURE REVIEW

In 2020, Yu et al. [1] have proposed an encryption for image algorithm on the basis of the phase-truncated short-time fractional Fourier transform (PTSTFrFT) and the hyper-chaotic system. Here,the original image is split into 4 sub-images for independent image encryption. They have encoded these sub-images with encryption unit (EU) that was constructed from wave-based permutation. Then for ensuring the integrity of image information as well as for nonlinearity of phase truncation they have linked the phase information with amplitude information. The experimental evaluation of the projected model had revealed better key space and high sensitivity.

In 2019, Wang et al. [2] have introduced an innovative medical image encryption method on the basis of modified genetic algorithm (MGA) and coupled map lattices. Initially, the authors have generated the secure cipher-images with the aid of the coupled map lattice and have considered the count of the cipher-images as the initial value. Then, with this initial population they have initialized the MGA. As a result, the computational time was lessened and entropy of the cipher-images was improved.

In 2019, Thoms et al. [7] have developed an image encryption algorithm referred as Chaos Net, It uses key based neural networks for integration with the roadside units of ITSs. The cryptanalysis shoes that the proposed method has good mixing properties and provides good information entropy.

In 2018, Nematzadeh et al. [8] have introduced an image encryption algorithm with random diffusion based on the spatiotemporal chaos of the Logistic-dynamic mixed linear-nonlinear coupled map lattices (LDMLNCML). The proposed LDMLNCML system had possessed important features of cryptography. The proposed image algorithm had adopted the theory of random diffusion. On the basis of the image pixels, the authors have generated the pending sequence and they have combined the conflict handling process to generate two index chains. Finally, the cipher image was acquired by random diffusion.

VIII. COMPARATIVE ANALYSIS OF OPTIMIZATION ALGORITHM FOR IMAGE ENCRYPTION

Author [Citation]	Methodology	Features	Challenges
Yu *et al*. [1]	PTSTFrFT	✓ Sensible to key ✓ Robust against the common attacks ✓ Resists chosen-plaintext attack	× Exhibits weaker correlation among pixels of encrypted image.
Wang *et al*. [2]	MGA	✓ Secure against brute-force attack ✓ Low computational time	× Do not have essential key space × The quality of decryption images are low
Thoms *et al*.[3]	Lorenz chaotic system	✓ Robustness to cropped attacks	× High entropy
Nematzadeh *et al*. [4]	LDMLNCML	✓ Reduce the correlation between the ✓ Adjacent pixels possesses good chaos ✓ High-sensitivity image encryption algorithm	× High noise intensity

IX. BENCHMARKS FOR OPTIMIZATION TEST

A. Key Sensitivity Analysis

The efficiency of an image encryption algorithm will be calculated depending on different cipher images it produces for the chosen key values. Any Encryption algorithm should be sensible to the key value chosen as the parameter for the encryption algorithm. It should result in different cipher images for a minute change in the key parameter.

B. Histogram Analysis

Quality of the cipher image is analyzed by the histogram generated by the cipher image. A good cipher image generates random like image which generates uniformly distributed histogram. Thereby making the cipher image far different from the input plain image.

C. Adjacent Pixel Auto-Correlation Test

Cipher image should possess low correlation among adjacent pixels. Pixel information redundancy is the general format of the plain image. The cipher image generated from the good image encryption algorithm should exhibit low correlation among its pixels.

D. Information Entropy Test

Randomness of an image is deduced by Information Entropy test. The scores of means and variances indicate the randomness in the cipher image. The output of the encryption algorithm generates diverse values for information entropy measurement.

E.UACI & NPCR Tests

The encryption algorithm should produce the cipher image with high resistance to differential attacks. Unified average changed intensity (UACI) and The number of changing pixel rate (NPCR) values judge how resistant the cipher image for differential attacks.

X. X. RESULTS AND COMPARISON

A.Correlation Coefficient Analysis

Table 1.Tabulation for Standard Correlation

Horizontal Direction	Vertical Direction	Diagonal Direction
-0.008131	-0.001382	-0.001016
-0.007393	-0.005329	0.000608
0.004851	-0.002044	-0.0027
0.001194	0.003131	-0.001784
-0.002569	0.000198	-0.002134
0.92387	0.90037	0.87506
0.0079	-0.0005	-0.0044
-0.0012	0.0095	-0.0093

Cipher image after encryption process is expected to show adverse correlation among pixels. SeaLion algorithm provides good cipher image which is not vulnerable to any type of attack.

B. Key Sensitivity Analysis

Table 2. NPCR Values of Encryption Images					UCAI Values of Encryption Images			
Max (%)	Min (%)	Mean (%)	Pass Rate(%)		Max (%)	Min (%)	Mean (%)	Pass Rate(%)
99.66	99.57	99.61	100		33.64	33.36	33.48	100
99.66	99.56	99.22	100		33.64	33.28	33.47	100
99.66	99.55	99.82	99.22		66.61	33.28	33.45	100
					Table3: UACI Values			

Encryption algorithm will be able to produce strong cipher image only with the strong encryption key. Key sensitivity is analysed by measuring NPCR and UACI values. The strength of the proposed SeaLion algorithm lies in producing very highly sensible key.

XI. CONCLUSION

The current research work proposes an O2DCM for encrypting the image data. Image Security is analysed using the benchmarks of the optimization algorithms. The proposed SeaLion optimization algorithm improves information entropy by using the new key generation strategy of the proposed algorithm.

REFERENCES

1. Cha-Cha Yu, Nan-Run Zhou, Li-Hua Gong, Zhe Nie,"Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system",Optics and Lasers in Engineering, vol.124, January 2020
2. Xingyuan Wang, Hongyu Zhao, Le Feng, Xiaolin Ye, Hao Zhang,"High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices",Optics and Lasers in Engineering, col.122,pp225-238,November 2019
3. Wang Xingyuan, Zhang Junjian, Cao Guanghui,"An image encryption algorithm based on ZigZag transform and LL compound chaotic system",Optics & Laser Technology,vol.119,November 2019
4. C. Zhu and K. Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps," in IEEE Access, vol. 6, pp. 18759-18770, 2018.
5. X. Zhang and X. Wang, "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem," in IEEE Access, vol. 6, pp. 70025-70034, 2018.
6. M. Guan, X. Yang and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," in IET Image Processing, vol. 13, no. 9, pp. 1535-1539, 18 7 2019.
7. G. R. W. Thoms, R. Muresan and A. Al-Dweik, "Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems," in IEEE Access, vol. 7, pp. 158697-158709, 2019.
8. ossein Nematzadeh, Rasul Enayatifar, Homayun Motameni, Frederico Gadelha Guimarães, Vitor Nazário Coelho,"Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices",Optics and Lasers in Engineering, Vol.110,pp.24-32,November 2018

ACKNOWLEDGMENT

The authors thank the management of Hindustan Institute of Technology and Science for rendering their continuous support, encouragement and cooperation throughout the progress of the work.

AUTHORS PROFILE

Latha H R, Assistant Professor,Dept. of Computer Applications,Jindal College for Women, Bangalore, Karnataka,India.Research Scholar, Hindustan Institute of Technology and Science, Chennai.

Dr. A. Rama Prasath Assistant Professor (Selection Grade), Department of Computer Applications, Hindustan Institute of Technology and Science, Chennai, India. His research interests are in the area of evolutionary algorithms, image processing and wireless network.