IMAGE ENCRYPTION SCHEME BASED ON DNA ENCODING AND BINARIZED CHAOTIC CORES

[1]**Dr. G. Nagaraju,** Assistant Professor, Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
[2]**P. Udaya Bhanu,** Assistant Professor, Department of EEE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
[3]**V.Swetha,** B. Tech Student, Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
[3]**T.N.V.Surya Teja,** B. Tech Student, Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
[3]**SK. Davood Saleem,** B. Tech Student, Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
[3]**S. Varun Naidu,** B. Tech Student, Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.
Corresponding author: [1]bhanu.raj.nikhil@gmail.com, +91 9010133466

Abstract: One-dimensional (1D) chaotic maps suffer from a restricted number of control parameters and convergent periodicity under finite precision implementation, making them unsuitable for hardware-based despite their straightforward implementation and affordable technology, ciphering systems [1]. The limited periodicity of 1D maps under fixed point precision representation is initially covered in this study. Following that, a picture encryption scheme based on DNA encoding and two uniquely configured binarized chaotic cores is shown. The purpose of both cores is to generate pseudorandom numbers that have great cryptographic qualities to carry out the confusion and diffusion stages of the image. By transforming both the chaotic stream and the image to DNA sequences according to a predefined DNA encoding rule, DNA encoding gives the method an additional layer of protection. Based on a computed hamming distance, the initial values of both chaotic cores depend on the image. All security analyses performed on the scheme showed that it could withstand known assaults with excellent encryption qualities, provided that all computations used in the scheme are based on binary integer arithmetic.

Keywords: Chaos, DNA computing, DNA encoding, image encryption, cyber security, entropy, NPCR, UACI

1. INTRODUCTION

Reliance on technology has become an integral part of our daily lives in the modern world. Due to this reliance, more sensitive information is now handled via communication networks and cloud storage services [11]. As a result, cryptographers realized how critical it was to advance security methods to shield this information from hacker attacks and illegal access. Typically, ciphering data calls for a decryption technique, a key to encrypt/decrypt the ciphered data, in [2, 4] G. Naga Raju proposed the concept of alphanumeric secret keys, a communication channel for data transfer, and an encryption scheme. The fundamental elements of a ciphering system are shown in Fig. 1

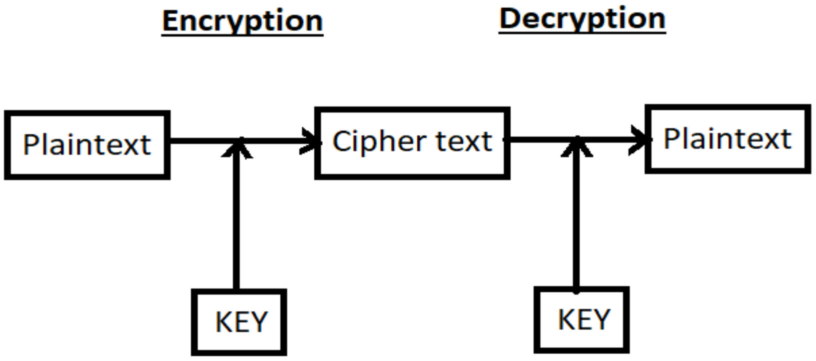


Fig. 1: Fundamental elements of a ciphering system

The key's characteristics, such as secrecy, improbability, and resistance to exhaustive search (brute force assault), are what primarily determine the strength of an encryption system. In an "unbreakable" scheme, according to Shannon, a key must have the same length as the message, be truly random, and only be used once (also known as a one-time pad, or OTP). However, some of these characteristics ultimately turned out to be unfavorable, as it makes more sense to send the message itself through a secure link than to share a key over such a vast distance. Additionally, if the same key is used again, an attacker may be able to decipher the messages using a basic running key cipher created by simple XOR or frequency analysis.

The OTP's impracticality made it possible to develop stream generators, which generate lengthy random sequences from relatively short seeds. These random number generators (RNG) can be divided into two categories: true (TRNG) and pseudo (PRNG), the latter of which is deterministic and based on methods that generate a sequence with characteristics that resemble those of true random numbers. Because of its sensitivity to initial conditions, evenly dispersed output, and uncorrelated long sequences, chaos based PRNG are currently in use widely. Furthermore, discrete chaotic functions are simple to implement on currently available modules and are hardware friendly.

1.1 RELATED WORK

Given their deterministic nature and random-like behavior, chaotic systems are a primary source of RRN in the most recently suggested ciphering algorithms. However, identical mathematical representations or hardware implementations of these chaotic cores are needed to regenerate the same sequence in both ends of the channel. Recent thorough research showed how finite precision affected several 1D chaotic systems' periodic characteristics. Elmanfaloty and Abou-Bakr demonstrated the effectiveness of fixed-point representation in terms of hardware resources and latency from a hardware standpoint and is shown in Fig. 2

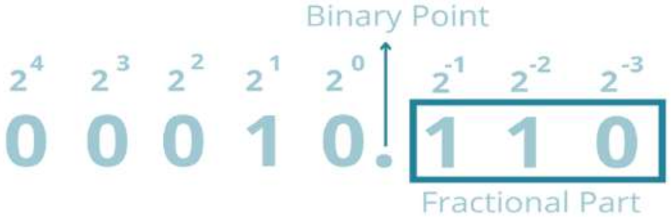


Fig. 2: Fixed point representation of binary numbers

1.1.1 BINARISZATION OF 1D CHAOTIC MAP

The method of performing all arithmetic operations using the base-2 representation is known as Binarization of 1D chaotic maps. The binary equivalents of addition, subtraction, multiplication, and division are included here. Hardware-wise, addition, shifting, and negation are used in tandem to implement subtraction, multiplication, and division. This section of the study briefly reviews the impact of utilizing fixed point representation to create several of the 1D chaotic maps, specifically the logistic map, tent map, and skew-tent map. Binary numbers can be expressed as t-bit integer parts and q-bit fraction parts, as shown in Fig. 2.

All mathematical operations on these maps are carried out with $t = 4$ bits and q with variable size throughout this study to examine the impact of q bits length on the periodicity of the output sequence. All of the aforementioned binary operations were carried out on a PC using Matlab to speed up testing and obtain results that resembled hardware implementation. The truncation rule applies to multiplication and division results.

A. LYAPUNOV ENTITY

A chaotic system is primarily identified by its topological transitivity, sensitivity to beginning conditions, and dense periodic orbits. Calculating the system's Lyapunov exponent (LE) and testing for convergence or divergence between two significantly perturbed trajectories are two standard techniques for figuring out the sensitivity to initial conditions:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \frac{|\delta_1|}{|\delta_o|} \qquad (1)$$

where the two trajectory spacings are 1 and 2 and stands for the LE. If all other circumstances are satisfied, > 0 typically denotes chaos. The parameters of various maps are shown in Table.1.

MAP	PARAMETERS	
Logistic map	r = 4	X_0 = 0.25
Tent map	µ = 2	X_0 = 0.25
Skew-tent map	P = 0.4	X_0 = 0.25

Table 1: Parameters used to generate graphs in Fig. 4

B. TENT MAP, SKEW-TENT MAP, AND LOGISTIC MAP

The logistic map [20] is a classic illustration of a straightforward discrete equation with distinctive chaotic features. Robert May, a biologist, initially presented the map in 1976. The second-degree equation that describes it is given by:

$$x_{n+1} = r^* x_n(1- x_n) \qquad (2)$$

The logistic map's bifurcation diagram and LE curve are shown in Fig. 3. It is clear from the map that at r = 4, LE > 0 in the overall state space and full pandemonium are present. The bifurcation diagram and LE might both provide the same visual results if the map in (2) is binarized and implemented using fixed point notation. However, Fig. 4 shows erroneous LE results and a limited periodicity in the bifurcation diagram when the logistic map is implemented using q = 4, 8, 16, 32 bits and the Table.1 parameters. It should be noted that LE alone does not indicate chaos; rather, it only shows how sensitive a system is to its starting conditions.

However, LE is the typical test for determining if a topologically mixed system exhibits chaotic behavior. However, the system's periodicity is highly dependent on the underlying limited precision. The periodicity of the logistic map (2), tent map (3), and skew-tent map (4) are plotted against q, however these sequences were found to have poor cryptographic properties, making them unfit for use in safe ciphering systems. The settings used to create the graphs in Fig.4 are listed in Table.1.

$$x_{n+1} = \begin{cases} \mu x_n & x \in \mathbb{R} : x \in [0, 0.5] \\ \mu(1 - x_n) & x \in \mathbb{R} : x \in (0.5, 1] \end{cases} \qquad (3)$$

$$x_{n+1} = \begin{cases} \frac{x_n}{p} & x \in \mathbb{R} : x \in (0, p] \\ \frac{1-x_n}{1-p} & x \in \mathbb{R} : x \in (p, 1) \end{cases} \qquad (4)$$

Where p ∈ (0,1).

1.1.2 DNA COMPUTING

Any reliable picture encryption technique must have the common traits of image pixel confusion and diffusion; G. Naga Raju in [8] proposed it as the chaotic process. The suggested approach uses two chaotic systems cores and DNA encoding [1] to satisfy these requirements and create a ciphered image that can withstand known attacks. In 1994, Leonard Adleman invented this field by utilizing DNA to solve a seven-point Hamiltonian path problem. As a type of computing device, sequences. Since then, DNA computing has outperformed more conventional techniques thanks to its vast storage capacity, ability for parallel processing, and low power usage. Deoxyribonucleic acid (DNA), in biology, is made up of two helical strands called polynucleotides, each of which is made up of less complex monomeric units called nucleotides.

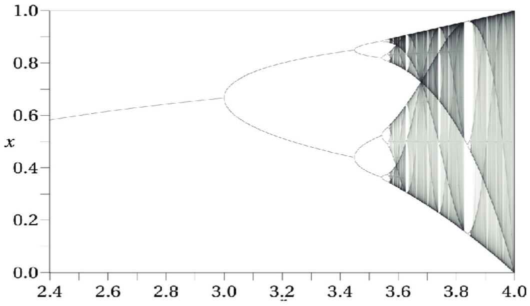
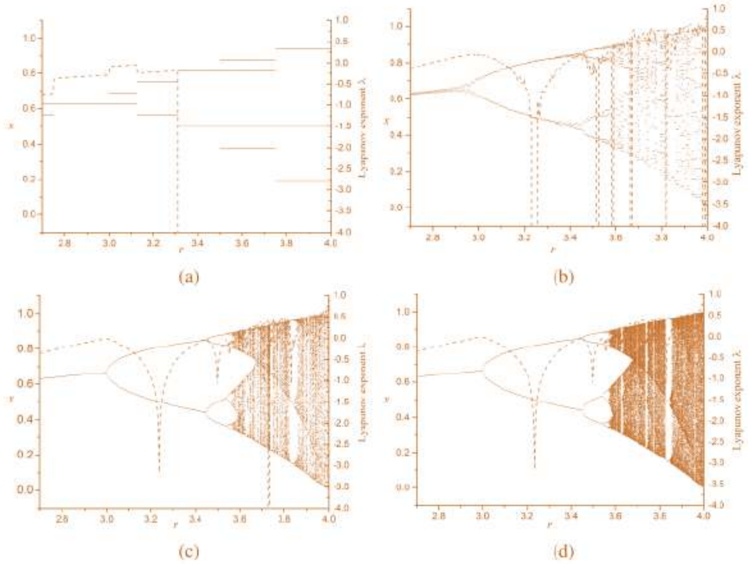


Fig. 3: Bifurcation diagram (blue) and LE (dashed red) for different values of r in the logistic map.

DNA RULE	A	T	C	G
Rule 1	00	11	01	10
Rule 2	00	11	10	01
Rule 3	01	10	00	11
Rule 4	01	10	11	00
Rule 5	10	01	00	11
Rule 6	10	01	00	11
Rule 7	11	00	01	10
Rule 8	11	00	10	01

Table 2: DNA Encoding Rules

Any one of these nucleotides is built from one of four nucleobases that include nitrogen: "C" cytosine, "G" guanine, "A" adenine, and "T" thymine. Because "A" is the complement of "T," "C" is the complement of "G," and vice versa, these nucleotides are distinguished by their complimentary pairing. Each nucleotide is represented by two bits in DNA computing, which follows the complementary rule. For instance, if "A = 00," then "T = 11," and if "C = 10," then "G," respectively.



(a) (b) (c) (d)

Fig. 4: Effect of fixed-point precision (binary fraction) on the bifurcation diagram and LE of the logistic map, (a) 4-bit fraction, (b) 8-bit fraction, (c) 16-bit fraction and (d) 32-bit fraction.

This means that only 8 out of the 24 DNA rules, as shown in Table.2, fulfill this complementary pairing. To use DNA computing, the sequence must be subjected to several logical and algebraic equations. Fig. 6 shows some of these operations for DNA sequences that fall under the first rule. As a result, each of the remaining eight rules has its own special table for logical and algebraic operations.

Since an image's pixels are each represented by 8 bits, they can all be converted using one of the DNA encoding rules into 4-character DNA sequences. For instance, according to the first rule, a pixel with a value of 224 ('11110100b') would be translated into the DNA code for "TTCA".

1.1.3 HAMMING DISTANCE

Hamming distance [1], in general, determines how many slots there are for various symbols in two strings of identical length. Using the following equation, this study makes use of this property to determine bit wise position differences in equally sized blocks of the image:

$$\begin{cases} H(x,y) = \sum_{1}^{n} h(x_i, y_i) \\ h(x_i, y_i) = \begin{cases} 0, & x_i = y_i \\ 1, & x_i \neq y_i \end{cases} \end{cases} \qquad (5)$$

The hamming distance is exploited throughout the encryption process in both the confusion and diffusion stages by changing the parameters and beginning values of the two chaotic systems, which makes them reliant on the plain picture.

2. PROPOSED METHODOLOGY:

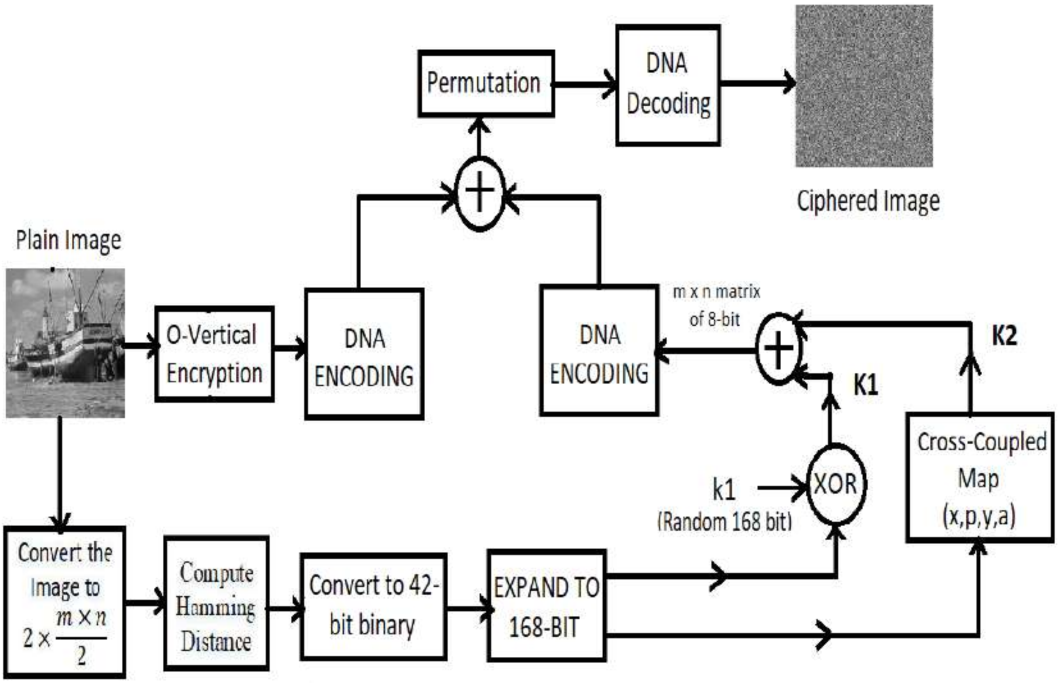
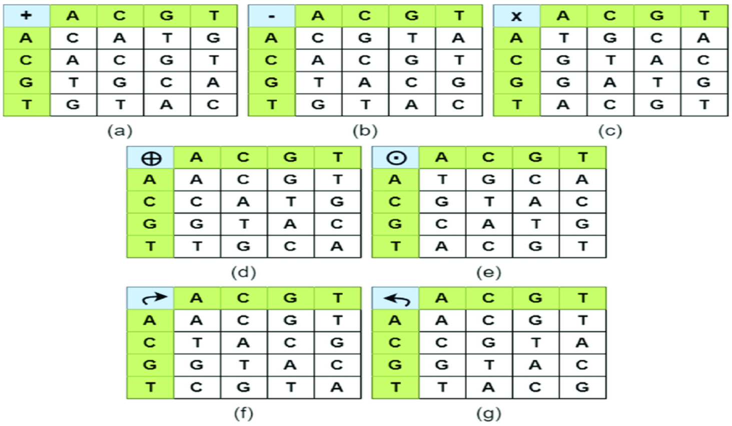


Fig. 5: Block diagram of the proposed algorithm

The suggested approach shown in Fig. 5 has two chaotic cores as proposed by G. Naga Raju in [2], one for the permutation process and the other for pixel confusion. Previously proposed chaotic systems are used to implement each core. The PRNG is fully binarized and is composed of two crossed coupled skew tent maps [3]. Its logical and algebraic operations all use fixed point representation. The result is an n-bit stream that has undergone numerous statistical tests to demonstrate its cryptography and randomization features. The system's output in this study is purposefully created to provide an 8-bit stream, making it appropriate for immediate use in picture encryption techniques, A 336-bit secret key made up of "K1, K2" will be transmitted.

2.1 DNA OPERATIONS:



+	A	C	G	T
A	C	A	T	G
C	A	C	G	T
G	T	G	C	A
T	G	T	A	C

(a)

-	A	C	G	T
A	C	G	T	A
C	A	C	G	T
G	T	A	C	G
T	G	T	A	C

(b)

x	A	C	G	T
A	T	G	C	A
C	G	T	A	C
G	G	A	T	G
T	A	C	G	T

(c)

⊕	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

(d)

⊙	A	C	G	T
A	T	G	C	A
C	G	T	A	C
G	C	A	T	G
T	A	C	G	T

(e)

↷	A	C	G	T
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C
T	C	G	T	A

(f)

↶	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

(g)

Fig. 6: DNA algebraic operations (a) ADD, (b) SUB, (c) MUL, (d) XOR, (e) XNOR, (f) Right circular shift, (g) Left circular shift.

2.1.1 KEY STRUCTURE:

For the first skew-tent map, each core needs p, xo, and for the second, a, y_o, to work. These parameters are represented for each map by a binary sequence of 168 bits, which creates the major secret keys K1 and K2. Additionally, the hamming distance for the plain picture is calculated and transformed to a 168-bit stream to make these keys dependent on the plain image in the encryption side. By XORing the 168-bit estimated hamming distance with another secret key, "k1, K2," the "K1, K2" stream also gains an additional layer of protection. The length of the overall A 336-bit secret key made up of "K1, K2" will be transmitted.

2.1.2 ENCRYPTION PROCEDURE:

During the encryption process, the following steps are taken:

1) Read plain images.
2) Calculate the hamming distance.
3) Convert the calculated hamming distance to 168-bit.
4) XOR the 168-bit hamming code with a secret Sub-key k1 and generate K1 for the first chaotic core.
5) By using the cross coupled map (by coupling two skew tent maps), generate a sequence called K2 and perform XOR between K1 & K2.
6) Run the first Chaotic core to generate an m × n matrix of 8-bits.
7) Encode the plain image with a DNA encoding rule after applying O_Vertical encryption technique to it.
8) Encode the matrix of the first chaotic System with the same DNA encoding rule.
9) Perform a DNA Addition operation. Second: the permutation stage.
10) Permute the output result of stage (9) using the extracted sequence.
11) Perform DNA decoding using the selected DNA-rule.

To avoid any association between the sequences for the confusion and diffusion stages, it was decided to use two cores. The opposite of the encryption process is the decryption procedure and is exactly as reverse of the encryption process.

3. RESULTS:

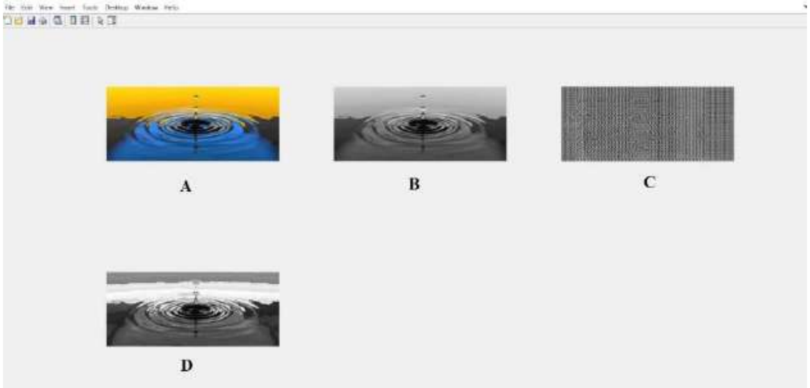


Fig. 7: Image-1

In Fig. 7 ‘A’ shows the input colour image and ‘B’ shows the gray scale image of ‘A’. By applying our proposed algorithm on ‘B’ we obtained an encrypted image which is shown in ‘C’. And the decrypted image of the above encrypted image is shown in ‘D’.

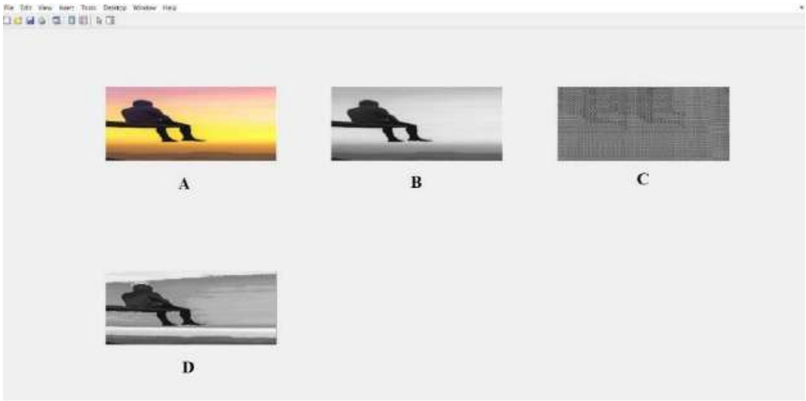


Fig. 8: Image-2

Similarly, in Fig. 8 ‘A’ is the input colour image and is converted to gray scale image ‘B’ and we applied the same algorithm as the above image we get Encrypted image ‘C’, and its decrypted image is ‘D’.

PARAMETERS:

IMAGE	NCC	MSE	NPCR	UACI	PSNR
Lena	0.8945	1.0780e+03	94.7943	7.3568	37.8046
Water	0.8122	1.8926e+03	92.0195	7.9196	35.3603
Colours	0.8084	2.6191e+03	98.7557	6.4514	33.9493
Sunset	0.9087	304.3541	85.0205	3.2537	43.2970
Boat	0.8697	1.5087e+03	93.9795	7.9990	36.3449
Sky	0.9122	678.8162	87.7371	3.7463	39.8133

Table 3: Comparison between input image and decrypted image

Table 3 represents how close the input image and the decrypted image are**.** The NCC parameter represents the correlation between them, MSE represents mean square error, NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified, PSNR represents the peak signal-to-noise ratio, UACI measures the average changing in intensity between original and ciphered images.

IMAGE	BER	NPCR
Water	0.4956	99.5275

Colours	0.5064	99.7514
Sunset	0.4970	99.7690
Lena	0.4845	99.3729
Boat	0.4980	99.5338
Sky	0.4741	99.4310

Table 4: Comparison between input image and encrypted image

Table 4 represents how different the input image and the encrypted image are. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval.

4. CONCLUSION

This paper presents a novel image encryption scheme based on DNA and binarized chaotic cores. The scheme was subjected to multiple statistical and security analysis, all of which provide its robustness and ability to withstand known attacks. In the future we can encrypt images with much better accuracy by developing this model.

REFERENCES:

[1] Rania A. Elmanfaloty, Abdullah M. Alnajim, AND Ehab Abou-Bakr,"A Finite Precision Implementation of an Image Encryption Scheme Based on DNA Encodingand Binarized Chaotic Cores,"IEEE ACCESS, VOLUME .9, pp. 136905-136916, 2021.

[2] G. NAGARAJU and T. V. HYMA LAKSHMI," Image Encryption using Secret-Key images and SCAN Patterns," Int. J. of Advances in Computer, Electrical & Electronics Engg., Vol. 2, Sp. Issue of NCIPA 2012, pp.13-18, December.2012.

[3] R. A. Elmanfaloty and E. Abou-Bakr, ``An image encryption scheme using a 1D chaotic double section skew tent map," Complexity, vol. 2020, pp. 1-18, Oct. 2020.

[4] Ramaraju PV, Nagaraju G, Chaitanya RK.,"Image Encryption and Decryption using Advanced Encryption Algorithm," *Discovery*, Vol.29(107), pp. 22-28, 2022.

[5] R. A. Elmanfaloty and E. Abou-Bakr, ``Random property enhancement of a 1D chaotic PRNG with finite precision implementation," Chaos, Solitons Fractals, vol. 118, pp. 134-144, Jan. 2019.

[6] G. Naga Raju, Dr. P.V.Rama Raju, P.Sai Priyanka, M. Mohan Krishna, M.S.V.Sravya, N.Hema Sai Kumar," STEGANOGRAPHY WITH LSB BINARY ADDITION," Journal of Emerging Technologies and Innovative Research (JETIR).,Volume.4,Issue 11,pp 138-142,November.2017.

[7] I. Öztürk and R. Kiliç, ``Cycle lengths and correlation properties of finite precision chaotic maps," Int. J. Bifurcation Chaos, vol. 24, no. 9, 2014, Art. no. 1450107.

[8] G. Naga Raju, Dr. P V Rama Raju, R.L V S S Subbarayudu, K. Maa Lakshmi, R. S S Vidya Sagar and T.Parimala,"Image Encryption Using Chaotic Process," International Journal of Trend in Research and Development, Volume .4(6),pp 6-9,Nov-Dec.2017.

[9] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, ``Local Shannon entropy measure with statistical tests for image randomness," Inf. Sci., vol. 222, pp. 323-342, Feb. 2013.

[10] G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, "A New Watermarking Scheme for Medical Images with Patient's Details," International Journal of Engineering & Technology, vol.7(3.31), pp 25-29,2018.

[11] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, ``Advances in security and privacy of multimedia big data in mobile and cloud computing," Multimedia Tools Appl., vol. 77, no. 7, pp. 9203-9208, Apr. 2018.

[12] G.Nagaraju, M.Venkata Pullarao , Dr.P.V. Ramaraju,"A Compound Transform Domain based Watermarking Scheme for Colour Images,"Jour of Adv Research in Dynamical & Control Systems, Vol. 11, 01-Special Issue, 2019.

[13] P. L'Ecuyer, ``Random number generation," in Handbook of Computa-tional Statist ics. Berlin, Germany: Springer, 2012, pp. 35-71.

[14] G. Nagaraju, Dr. P.V. Ramaraju, P. UdayaBhanu, Y.S.V. Satyavathi, T. Srinadh, K. Ganesh, K. Hari Subrahmanyam, "Optimized Image Watermarking Scheme Based on IWT and DCT", International Journal of Advanced Science and Technology, Vol. 29, No. 4, (2020), pp. 132-147.
[15] G. Naga Raju, Dr. P V Rama Raju, P. Udaya Bhanu, P V V Abhilash, M S S S L Prasad,N Keerthi, P Satish,"A Hybrid Encryption Technique for Data Embedding in Medical Images,"International Journal of Advanced Science and Technology,Vol. 29, No. 4, (2020), pp. 116-131.
[16] G. Nagaraju, P. Pardhasaradhi, V.S. Ghali and Sateeshkumar Deevi, "An Intelligent Watermarking Technique for Secured Medical Images with Patient Health Document", The Journal of Research on the Lepidoptera, Volume 51 (3), pp.01-17, 2020.
[17] G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, G.R.K Prasad,"Secure Hybrid Watermarking Technique in Medical Imaging,"European Journal of Molecular & Clinical Medicine, Volume 07, Issue 05, pp.160-176,2020.
[18] Dr. G. Nagaraju, P. Udaya Bhanu, M. Vaishnavi, R. Ravi Teja, K. Sai Rohit, R. Vineel kumar,"Digital Image Security System Based on Logistic and Chebyshev Techniques,"Dogo Rangsang Research Journal, Vol-09 Issue-01 No. 01, pp. 1115-1123,2022.

ABOUT AUTHORS:

Dr. G. NAGA RAJU

Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.E. degree from S.R.K.R Engineering College, Bhimavaram in 2002, and M.E. degree in Computer electronics specialization from Govt. College of Engg., Pune University in 2004. PhD degree from Department of ECE, KL University, Vaddeswaram in 2021. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.

Mrs. P. UDAYA BHANU

Presently working as assistant professor in Dept. of EEE, S.R.K.R. Engineering College, Bhimavaram, AP, India. She received B. Tech degree from DNR College of Engineering and Technology, Bhimavaram in 2016, and M. Tech degree in Power Systems and Automation specialization from S.R.K.R Engineering College, Bhimavaram in 2018. Her current research interests include Signal processing, Image processing, Power systems and Automation.

V. SWETHA

Currently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College (A), AP, India.

T. N.V. SURYATEJA
Currently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College (A), AP, India.

SK. DAVOOD SALEEM
Currently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College (A), AP, India

S. VARUN NAIDU
Currently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College (A), AP, India.