AN NOVEL IMAGE ENCRYPTION SCHEME BASED ON DNA COMPUTING AND CHAOTIC SYSTEMS

Chittoori Brahmaji [1], M.Tech, Student, Dept. of ECE, Eluru College Of Engineering and Technology, Jntuk
Kinnera Ravi kumar [2], M.Tech, Assistant Professor, Dept. of ECE, Eluru College Of Engineering and Technology, Jntuk

Abstract

A wide variety of strategies for securing plaintext, images and video frames have been evolved in cryptography the usage of mutually DNA computing and Chaos Theory. With the advancement of DNA/quantum computing, the threats of safety breaches to data have an growing possibility. In this paper, we advocate a symmetric encryption algorithm for color pix by using extending the modern-day encryption/decryption techniques. Our encryption set of rules is based on three chaotic structures (PWLCM, Lorenz and 4D Lorenz-type), a Secure Hash Algorithm, a scrambler, a chaotic generator and DNA series primarily based Linear Feedback Shift Register. We introduce multilevel safety to growth the diploma of diffusion and confusion. Through experiments, we gift safety evaluation for key irreproducibility and sensitivity, Gray Level Co-occurrence Matrix based analysis, most deviation, irregular deviation, entropy, histogram, variance and correlation, number of pixel alternate price, unified common cipher depth, acknowledged/chosenplaintext attacks, mean absolute error, robustness in opposition to noises of diverse kinds the use of PSNR and occlusion assaults. It is established that mainly our proposed encryption algorithm has more suitable performance as compared to contemporary works in statistics safety, while similar in different instances.

Index Terms

Bit scrambling, chaotic generator, DNA encoding, hyper chaos, secure hash algorithm.

I.INTRODUCTION

The importance of facts security is increasing with digitization. Cryptography plays a vital function in confidentiality, integrity and availability of records. With developing computability, the digital protection stakes are higher than ever. A sturdy safety is needed to tackle statistics cracking. DNA (Deoxyribo Nucleic Acid) and chaotic device primarily based joint cryptography is an emerging area because of achieving new degrees of security, mainly that of color images and videos.. It is an extended polymer inclusive of small gadgets of nucleotides, with each nucleotide made of nitrogenous base, 5-carbon sugar and at the least one phosphate organization. Depending upon the type of nitrogenous base, there are four exclusive nucleotides known as adenine

(A), cytosine (C), guanine (G) and thymine (T) [1]. Pairs of these bases are related to every different in particular sequences via hydrogen bonds, therefore preserving the 2 strands connected. A gene is a awesome series of nucleotides that consists of genetic statistics of all living organisms. DNA computing in the direction of information protection is promising. Digital DNAs to be had from public genetic databases have billions of nucleotides, therefore enable a big space with an extended uncertainty. If used effectively by following the DNA sequencing, synthesis, recombination and hybridization operations, it leverages era of robust cryptographic keys. DNA based totally cryptography benefits from techniques which include One Time Pad (OTP), DNA fragmentation and DNA amplification through Polymerase Chain Reaction (PCR) [2]. Though cryptography strategies are majorly based totally on randomization, they have a tendency to be application vicinity unique. For example, plaintext may be encrypted the use of DNA microdots [3], [4], a method which isn't always at once applicable for securing images. Images can be encrypted by using processing them in a breadth first sample. The processing is based at the Chaos Theory and consists of scrambling, permutation, shuffling and dynamic diffusion [5], and 3-d permutation [6]. Other than breadth first pattern (row-clever), column-smart and diagonal-smart also are opportunities. Cryptography can be performed the usage of virtual watermarking, canny aspect detection and visualization [7]. DNA addition on a DNA encoded image and DNA matrix offers additive DNA. Visual encryption scheme is proven with the aid of transforming a undeniable photo into Visually Meaningful Encrypted Image (VMEI) the usage of a Logistic Map and a Gray S-Box [8]. Other than encrypting photographs offline, there's a opportunity of actual time encryption. For instance, in a stay conversation setup, encryption with a low computation overhead is possible using a chaotic map [9]. A distinctly secured encryption gadget can be done through combining chaotic systems and four cryptographic stages, specifically, diffusion based on XOR, substitution primarily based on S-boxes, diffusion based totally on a chaotic map and block permutation for reinforcement of the statistical results [10], [11]. Diffusion in multiple rounds based totally on bit permutation generator and bit diffusion generator has yielded promising encryption consequences [12]. Considering the development of DNA/quantum computing, it's miles increasingly turning into likely to breach exceedingly secured records, whether

it is textual content, photograph or films. Security strategies based on one or more than one chaotic structures mainly rely upon PWLCM (piecewise linear chaotic map) and Lorenz [5], [6], [10], [13]–[17]. To this stop, we purpose to preserve the protection intact as a good deal as almost possible. Motivated via picture encryption schemes and cryptanalysis [19], we make contributions by means of designing and proposing a symmetric picture encryption algorithm. It is based on three chaotic systems (PWLCM and Lorenz for variations, and 4D Lorenz-kind for key technology), a Scrambler for photo jumbling and DLFSR this is supported by a chaotic generator. It also makes use of a way to transform binary data to nucleotides bases and vice versa [20]. The proposed encryption algorithm fulfills the requirements of a robust cipher as pondered through its promising effects. The set of rules computes the preliminary hash the usage of a key space and provides this hash to the 3 chaotic structures to generate new initial situations. Using preliminary situations, PWLCM and Lorenz chaotic structures iterate on RGB additives individually, generating processed RGB components. The post processing key relies upon on two seed values. The first is a DNA seed taken from the NCBI database containing DNA sequences of animals or human genomes. It has additionally been used for watermarking the DNA sequences [21]. The 2d is a chaotic seed. Both seeds are fed to DLFSR and a chaotic generator, respectively. DLFSR and the chaotic generator give keys, which are XORed to get the very last key. The final key is XORed with the first stage encrypted picture to supply the final encrypted photo. Specifically, our contribution is more desirable safety performance, as established by using consequences. The rest of this paper is organized as follows. Section 2 incorporates the associated paintings. Section 3 offers our proposed algorithm and essential details explaining it. Section four consists of the results while our algorithm is carried out on some reference pictures and corresponding protection evaluation. Section 5 affords fundamental overall performance of our set of rules. Section 6 holds our final judgments and guidelines for destiny studies.

II.RELATED WORK

For consistency, we introduce our notation to represent all chaotic systems, whether they are referred to or our proposed.

HYPERCHAOS FOR SECURITY

Hyperchaotic systems show more randomness and unpredictability when compared with simple chaotic systems. We use 4D Lorenz-type [18], which is very

sensitive to initial conditions used for the key generation

$$\begin{cases} \dot{x}_1 = c_{1.1}\,(y_1 - x_1) \\ \dot{y}_1 = c_{1.2}x_1 - c_{1.3}y_1 - x_1z_1 \\ \dot{z}_1 = -c_{1.4}z_1 + x_1y_1 + w_1 \\ \dot{w}_1 = -c_{1.5}w_1 + c_{1.6}z_1. \end{cases}$$

(2) refers to the second hyperchaotic system in this paper. Low dimensional chaotic maps have small key areas main to low safety, at the same time as 4D hyperchaotic systems have big key space, producing a couple of chaotic sequences with unpredictable behaviour, a desired belongings to obtain high security [23]. A range of chaotic structures have been utilized in data security for securing gray and shade photographs. These encompass PWLCM, Chen's, Lorenz, different similar high dimension hyperchaotic structures, chaotic maps and double chaotic structures [5], [6], [10], [13]–[17]. Two chaotic systems (skew tent map and PWLCM) primarily based on decimal quantification had been widely used to improve the overall performance of photo encryption algorithms. Another method is defining diversifications based totally on cyclic organization properties for photo encryption in preference to a chaotic system [24] – [27]. Recent coloration photograph encryption algorithm proposals based totally on DNA and chaos have comparable outcomes [28], [29]. Availability of this records publically will assist concrete advancement within the subject of data protection.

DNA FOR SECURITY

Due to its immense space of sequences, DNA is well suited for achieving new levels of security in digital world. DNA is made up of four types of nucleotides called Adenin (A), Guanine, Cytosine (C) and Thymine (T). The nucleotides are linked together chemically and are the carrier of inherited traits. DNA exists in double stranded form twisted around each other, i.e., two strands of DNA are hydrogen bonded between complementary nucleotides, while the nucleotides within the strand are linked through phosphate [30]. Complementary nucleotides are AT and GC pairs. DNA rules [31] and DNA-XOR algebraic operation, shown in Table 2.1, can be used for DNA encoding and decoding. DNA based text and image security is significant though the computational complexity easily explodes with size of the DNA sequence. This issue is addressed by taking a 2-bit coding rule [10]. Diversity based boosting algorithm can be implemented in accurate classifications of DNA nucleotides of some specific length such as ACTTGGCTGT, AACCTCTGGG, etc., [32].

TABLE 1. XORing between DNA symbols [10].

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

DNA usage leverages a broad canvas of confusion and diffusion that can effectively enhance the robustness of a security algorithm. Any such approach can follow the DNA encoding rules, especially the dynamic DNA encoding rules combined with chaos [33]. Thus, the serious threats due to the promising DNA computing can be countered by powerful encryption schemes realized by DNA combined with chaotic systems. This is demonstrated by the resistance created against differential attacks due to a game based chaos method of diffusion in which keys based on DNA sequences are generated for image diffusion. Algebraic-Geometric (AG) codes [34] are still in their infancy stage, offering attractive applications in point to point communication and system security. DNA nucleotides may be replaced with AG codes to secure wireless communication systems from different attacks detected by different Intrusion Detection Systems (IDS). IDS are used to detect the attacks imposed by sharp attackers [35].

CHAOTIC GENERATOR AND LINEAR FEEDBACK SHIFTREGISTER / RANDOM BIT GENERATOR

"Randomness has a essential position in strengthening a safety mechanism. Unpredictability within the output of a random bit generator is a fundamental requirement in cryptography. Keeping the output of a random bit generator indeterministic is noticeably preferred despite the fact that its design is disclosed by some means. A aggregate of chaotic device and a couple of DNA regulations increases resistance to safety assaults [13]. We generate a very last submit processing key using our proposed random bit generator, DLFSR (primarily based on a real DNA series) and a chaotic generator (based on a floating-point seed price). Our chaotic generator uses Lorenz chaotic system for key series technology. The output of the chaotic generator and DLFSR are XORed to get the very last put-up processing key, f-key.

III.PROPOSED ALGORITHM

Here a symmetric key DNA prolonged chaotic encryption algorithm is proposed, hereafter called SDC-Encryption (SHA DNA Chaotic Encryption) that aims at enhancing the records protection (refers Algorithm SDC-Encryption). DNA is taken into consideration a excessive-velocity cryptography approach, that's appropriate to encrypt big volume of statistics . SDC-Encryption is implemented on plain

coloration photograph. Its flowchart is shown in Fig.1.

INITIAL CONDITIONS AND CHAOS

SDC-Encryption uses a chaotic system to growth randomness inside the encryption image. Let pI denote the plain RGB photo (m × n). Initial situations for the chaos are set as follows. The common of first row, first four pixel values, Algorithm SDC-Encryption Input:

Step 1: Choose the SHA based totally on the common cost of first 4 pixels of the plain color photo and generate new initial conditions.

Step 2: Take transpose of the plain coloration photo.

Step 3: Generate fake photographs (of same size as the plain shade image) and cut up them into their R, G and B components.

Step 4: The found R, G and B components are surpassed to a PWLCM system for iterations, producing three processed R, G and B additives which can be concatenated to form a processed photo whose pixel values are then looked after.

Step 5: Generate a brand new picture with the aid of permuting the pixel values of Step 2 photograph. Permutation is completed by considering the pixel values of Step 4 photograph as indices into Step 2 picture.

Step 6: Step five photograph is split into R, G and B components.

Step 7: Step 6 R, G and B additives are surpassed to a Lorenz chaotic machine, producing three R, G and B additives whose pixel values are then taken care of for my part.

Step eight: Generate 3 new R, G and B components by means of permuting the R, G and B components of Step 6. Permutation is completed by means of considering Step 7 issue pixel values as indices into Step 6 corresponding R, G and B additives. // Scrambling and key era

Step 9: A Scrambler feature maps every of Step 8 additives and corresponding keys to new R, G and B components. The corresponding keys are generated using Fourth Order Runge-Kutta method, a hyperchaotic device // DNA encoding.

Step 10: The R, G and B components of Step nine go through DNA collection encoding, which is based on DNA encoding rules, DNA complementing and DNA XORing. // DNA decoding

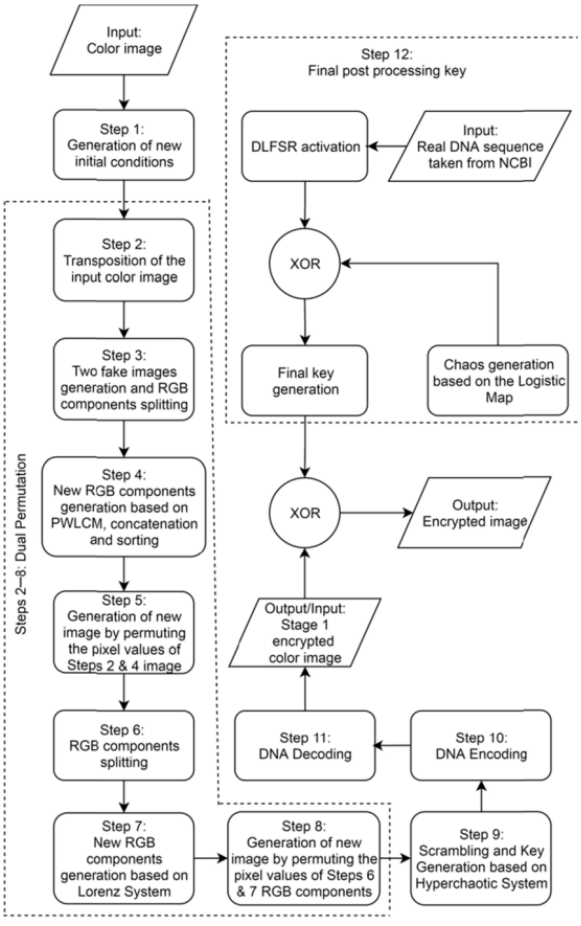

Fig 1. The flowchart of SDC-Encryption algorithm.

Step 11: Symbols within the DNA encoded chain of Step 10 go through DNA sequence interpreting. The result is considered as encrypted R, G and B components, which are concatenated to form an encrypted photo.
// Final submit processing key era

Step 12: The final post processing key, fkey, is generated by way of XORing the output of the Logistic Map based totally chaotic generator and DLFSR. The DLFSR is activated through the real DNA sequence. The encrypted picture of Step eleven is XORed with fkey to get the very last encrypted photograph.

DUAL PERMUTATION

We growth the randomness inside the obvious shade photograph with the aid of shuffling the pixels. Let the transpose of the apparent coloration photo. Now, generate faux images fI1 and fI2 of equal length as of pI and split them into their R, G and B additives, that are exceeded to PWLCM gadget for iterations generating three processed R, G and B components. Permutations are executed by means of thinking about the looked after pixel values as indices into. RI is cut up into R, G and B additives, which might be handed to a Lorenz chaotic system, producing three new R, G and B additives. Their pixel values are sorted personally and used as indices into the corresponding R, G and B components of rI to provide permuted R, G and B components, say, uR, uG and uB.

DNA ENCODING AND DECODING

DNA encoding and decoding is applied to a space that is generated using a scrambler function, mapping each of uR, uG and uB components and their corresponding keys to new R, G and B components, say uR0, uG0 and uB0 . The keys are mapped by fourth order Runge-Kutta method applied on (1) with c1.6 within [0, 9.5] to produce four chaotic sequences, which are combined into

a single array. DNA encoding on uR0, uG0 and uB0 is applied in three stages. DNA decoding is applied to the XORed output to obtain encrypted R, G and B components, which are concatenated to form first stage encrypted image, denoted by eI0 .

Corresponding to SDC-Encryption, we also propose a decryption algorithm, hereafter called SDC-Decryption (SHA DNA Chaotic Decryption), which is applied on an encrypted image to produce a plain color image

Algorithm Algorithm SDC-Decryption

Input: An encrypted image ($m \times n$).
Output: A decrypted image ($m \times n$).
Steps: Inverse steps of image encryption are carried out in the reverse order.

IV.RESULTS AND SECURITY ANALYSIS

We applied SDC-Encryption to four color images. A comparison between plain, encrypted and decrypted is shown in Fig.2. It is clearly noted that the encrypted images completely conceal information contained therein plain color images to keep maximum visual disparity. The decrypted images are almost replicas of the plain color images, reflecting minimal information losses, as also reflected by the peak signal-tonoise ratio (PSNR). PSNR can be defined in terms of mean squared error (MSE) between the plain image (m × n) and the encrypted/decrypted image (m × n). Denoting a processed (encrypted/decrypted) image by sI, we have

$$psnr(pI, sI) = 10log_{10}\left(\frac{MAX^2}{mse(pI, sI)}\right)$$

KEY IRREPRODUCIBILITY

Considering those primary obstacles together, the actual possibilities of a a success attack are tons smaller than the prevailing minimal probabilities 1 2 128 of protection. Increasing the forgery resistance as much as this degree is considerable, specifically against birthday attacks the ones may be accomplished by way of quantum computer systems. They can breach cryptographic protection structures by using locating the chance of collisions between random attack attempts at a few selected volumes of diversifications of a hash function.

KEY SENSITIVITY

A minor difference in the encryption key results in a significant modification in ciphertext. We tested the sensitivity of secret key of SDC-Encryption by encrypting the plain color image Knee (512×512) with the initial parameters and decrypting it with slight modifications in the initial parameters. The results shown in Fig. 7.3 clearly indicate absence of a relation between the plain color image and the decrypted image even after the initial conditions are slightly modified.

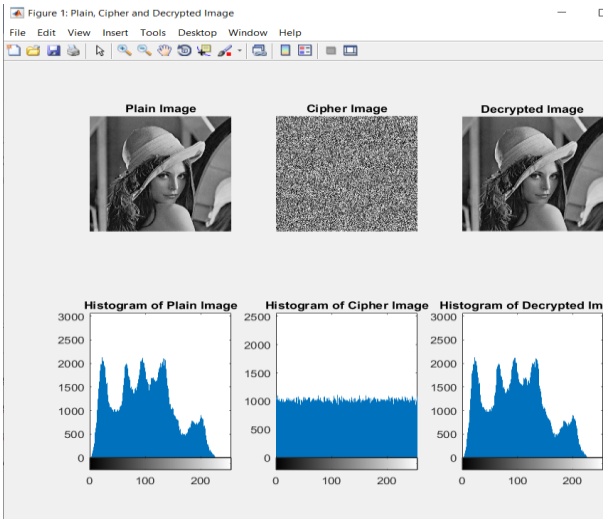

Fig 2. Plain, Cipher and Decrypted Ima

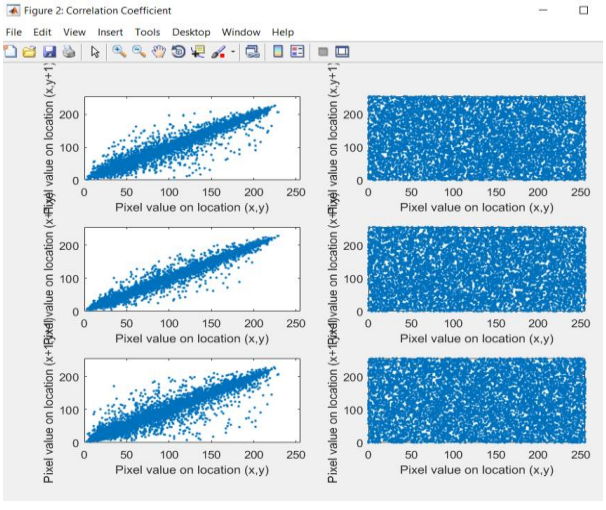

Fig.3. Corelation Coefficient Image

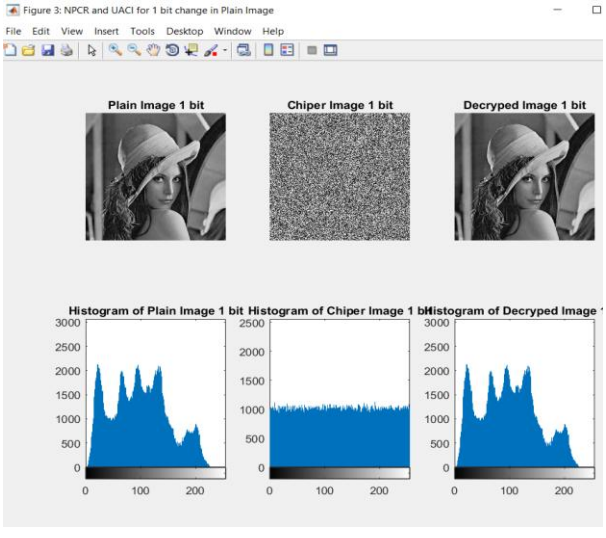

Fig.4. NPCR and UACI 1-Bit Plain

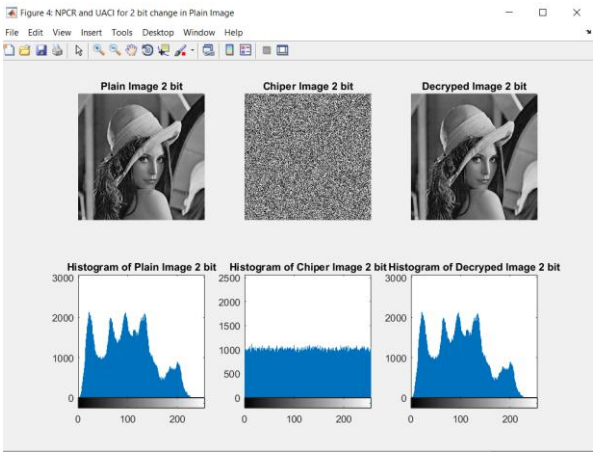

Fig.5. NPCR and UACI 2-Bit Plain Image

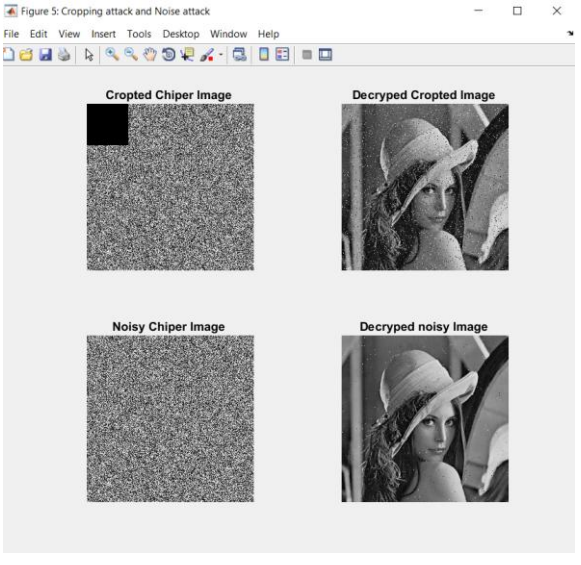

Fig.6. Cropping Attack and Noise Attack Image

Test Execution Time, Entropy and Correlation Coefficient ...

Encryption Time = 3.055233

Decryption Time = 2.619473

PlainImage - DecryptedImage = 0

PlainImage Entropy = 7.592929

CipherImage Entropy = 7.999317

Correlation Coefficient:

0.9728 -0.0165

0.9863 0.0034

0.9596 -0.0011

Test NPCR and UACI for 1 bit change in Plain Image...

Before change 1 bit of PlainImage at location (330,194) = 15

After change 1 bit of PlainImage at location (330,194) = 16

NPCR = 0.996197 UACI=0.334832

Test NPCR and UACI for 2 bit change in Plain Image...

Before change 2 bit of Plain Image at location (330,194) = 15

After change 2 bit of Plain Image at location (416,273) = 113

After change 2 bit of Plain Image at location (330,194) = 16

After change 2 bit of PlainImage at location (416,273) = 112

NPCR = 0.996185 UACI=0.334716

Cropping attack...

Crop=1/16, PSNR of cropped cipher image = 20.346853

Salt and pepper noise attack...

Noise Level = 0.005000, PSNR of nosiy cipher image = 31.423069

CONCLUSION

With the advancement of DNA/quantum computing, the present security mechanisms might not provide the required ranges of obstacles. There is a dire need to boost protection mechanisms through introducing more moderen techniques. Our experimental consequences are promising. We gift evaluation for key irreproducibility to assess the chances of duplicating the secret key as generated with the aid of our set of rules, key sensitivity, entropy, histogram, most deviation, irregular deviation, GLCM based evaluation, variance and correlation, variety of pixel exchange charge and unified average cipher depth, recognised/selected-plaintext assaults, suggest absolute mistakes, robustness towards noises of various kinds the use of PSNR and occlusion attacks. Better effects of safety analysis, resistance in opposition to multiple assaults, larger key area and sensitivity to chaotic secret keys reflect the significance and benefits of proposed scheme. It is demonstrated that mostly our proposed encryption set of rules has stronger performance compared to contemporary works in data safety, while similar in different cases. The computation complexity of our set of rules is determined to evaluate its feasibility in numerous use instances mainly that require run time encryption. The proposed algorithm time increases logarithmically for photos as much as (512×512) and exponentially beyond. In destiny we intend to have a look at vulnerability, weaknesses and optimization of computation complexity intensive operations to further improve the proposed technique and to house large shade pics

greater than or identical to (1024×1024). We additionally intend to introduce S-container and single or chaotic maps in preference to multiple chaotic maps in the future version of this paper.

REFERENCES

[1] I. Peterson, ‘‘Computing with DNA,’’ Sci. News, vol. 150, no. 2, p. 26, 2007.

[2] T. Anwar, S. Paul, and S. K. Singh, ‘‘Message transmission based on DNA cryptography: Review,’’ Int. J. Bio-Sci. Bio-Technol., vol. 6, no. 5, pp. 215–222, Oct. 2014.

[3] C. T. Clelland, V. Risca, and C. Bancroft, ‘‘Hiding messages in DNA microdots,’’ Nature, vol. 399, no. 6736, pp. 533–534, Jun. 1999.

[4] M. Rusia and R. H. Makwana, ‘‘Review on DNA based encryption algorithm for text and image data,’’ Int. J. Eng. Res. Technol., vol. 3, no. 1, pp. 3182–3186, 2014.

[5] Q. Yin and C. Wang, ‘‘Using breadth-first search and dynamic diffusion,’’ Int. J. Bifurcation Chaos, vol. 28, no. 4, pp. 1–13, 2018.

[6] X. Zhang and X. Wang, ‘‘Multiple-image encryption algorithm based on the 3D permutation model and chaotic system,’’ Symmetry, vol. 10, no. 11, p. 660, Nov. 2018.

[7] A. Fatahbeygi and F. A. Tab, ‘‘A highly robust and secure image watermarking based on classification and visual cryptography,’’ J. Inf. Secur. Appl., vol. 45, pp. 71–78, Apr. 2019.

[8] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, ‘‘Visual Meaningful Encryption Scheme Using Intertwinning Logistic Map,’’ in Intelligent Computing (Advances in Intelligent Systems and Computing), vol 857, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham, Switzerland: Springer, 2019.

[9] J. S. Khan and J. Ahmad, ‘‘Chaos based efficient selective image encryption,’’ Multidimensional Syst. Signal Process., vol. 30, no. 2, pp. 943–961, Apr. 2019.

[10] A. Belazi, A. A. A. El-Latif, and S. Belghith, ‘‘A novel image encryption scheme based on substitution-permutation network and chaos,’’ Signal Process., vol. 128, pp. 155–170, Nov. 2016.

[11] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, ‘‘Depreciating motivation and empirical security analysis of chaos-based image and video encryption,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[12] T. Gopalakrishnan and S. Ramakrishnan, ‘‘Chaotic image encryption with hash keying as key generator,’’ IETE J. Res., vol. 63, no. 2, pp. 172–187, Mar. 2017.

[13] P. Zhen, G. Zhao, and L. Min, ‘‘Chaos-based image encryption scheme combining

DNA coding and entropy,'' Multimedia Tools Appl., vol. 75, no. 11, pp. 6303–6319, Jun. 2016.

[14] K. Zhan, D. Wei, J. Shi, and J. Yu, ''Cross-utilizing hyperchaotic and DNA sequences for image encryption,'' J. Electron. Imag., vol. 26, no. 1, Feb. 2017, Art. no. 013021.

[15] K. A. K. Patro and B. Acharya, ''An efficient colour image encryption scheme based on 1-D chaotic maps,'' J. Inf. Secur. Appl., vol. 46, pp. 23–41, Jun. 2019.

[16] M. Annaby, M. Rushdi, and E. Nehary, ''Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion,'' Opt. Lasers Eng., vol. 103, pp. 9–23, Apr. 2018.

[17] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, ''Image encryptionthen-transmission using DNA encryption algorithm and the double chaos,'' IEEE Photon. J., vol. 10, no. 3, pp. 1–15, Jun. 2018.

[18] Y. Chen, ''The existence of homoclinic orbits in a 4D Lorenz-type hyperchaotic system,'' Nonlinear Dyn., vol. 87, no. 3, pp. 1445–14

[19] C. Li, Y. Zhang, and E. Y. Xie, ''When an attacker meets a cipher-image in 2018: A year in review,'' J. Inf. Secur. Appl., vol. 48, Oct. 2019, Art. no. 102361.

[20] M. Sabry, M. Hashem, and T. Nazmy, ''Three reversible data encoding algorithms based on dna and amino acids' structure,'' Int. J. Comput. Appl., vol. 54, no. 8, pp. 24–30, Sep. 2012.

[21] S. Hamad, A. Elhadad, and A. Khalifa, ''DNA watermarking using codon postfix technique,'' IEEE/ACM Trans. Comput. Biol. Bioinf., vol. 15, no. 5, pp. 1605–1610, Sep./Oct. 2018.

[22] A. Anees, ''An image encryption scheme based on lorenz system for low profile applications,'' 3D Res., vol. 6, no. 3, p. 24, 2015.

[23] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, ''A color image cryptosystem based on dynamic DNA encryption and chaos,'' Signal Process., vol. 155, pp. 44–62, Feb. 2019.

[24] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, ''An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers,'' Multimedia Tools Appl., vol. 77, no. 20, pp. 26191–26217, Oct. 2018.

[25] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, ''Image encryption using sequence generated by cyclic group,'' J. Inf. Secur. Appl., vol. 44, pp. 117–129, Feb. 2019.

[26] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, ''On the security of

permutation-only image encryption schemes,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 235–246, Feb. 2016.

[27] J. A. Alzubi, O. A. Alzubi, G. Suseendran, and D. Akila, ''+ A novel chaotic map encryption methodology for image cryptography and secret communication with steganography,'' Int. J. Recent Technol. Eng., vol. 8, no. 1C2, May, pp. 1122–1128, 2019.

[28] M. Sokouti and B. Sokouti, ''A PRISMA-compliant systematic review and analysis on color image encryption using DNA properties,'' Comput. Sci. Rev., vol. 29, pp. 14–20, Aug. 2018.

[29] F. Peng, X.-w. Zhu, and M. Long, ''An ROI privacy protection scheme for H.264 video based on FMO and chaos,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 10, pp. 1688–1699, Oct. 2013.

[30] L. Sharp, ''DNA sequencing and sorting: Identifying genetic variations,'' COMAP, Bedford, MA, USA, Tech. Rep., 2015.

[31] S. Hamad, ''A novel implementation of an extended 8×8 playfair cipher using interweaving on DNA-encoded data,'' Int. J. Elect. Comput. Eng., vol. 4, no. 1, pp. 93–100, 2014.

[32] J. A. Alzubi, ''Diversity-based boosting algorithm,'' Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 5, pp. 524–529, 2016.

[33] Z. Liu, C. Wu, J. Wang, and Y. Hu, ''A color image encryption using dynamic DNA and 4-D memristive hyper-chaos,'' IEEE Access, vol. 7, pp. 78367–78378, 2019.