Triple Image Encryption using Chaotic Maps and DNA Sequences

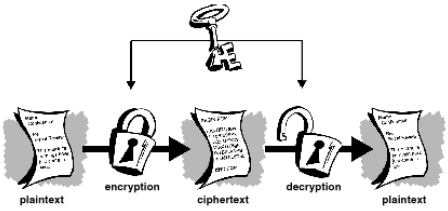
Y.S.V.Raman, A.Narendra Babu, M.Krishna Priyanka, Sk.Faria ,A.RamyaSree, G.Naga Prasanna,

Abstract*: With the fast advancement of system and data innovation, individuals are giving more consideration to the security of data, especially computerized picture insurance and various picture encryption calculations have been proposed. Image security problem can be solved efficiently and accurately using a technique: Bit-plane shuffling, DNA sequences for image encryption providing confidentiality and authenticity using SHA-256(Secure Hash Algorithm) and XOR of matrices using PWLCM method. This component will essentially increment plain text affectability. In addition, so as to achieve advanced safety and sophisticated intricacy, the future technique utilizes the picture estimate in important brook age course. The trial consequences uncover that the novel picture encryption calculation has the benefits of enormous important universe (256), tall safety, tall affectability (Amount of Pixels Change Rate: NPCR >99.6201 %, Unified Average Changing Intensity: UACI >33.5065 %), and high entropy (> 7.9975). Likewise, the dispersion of dim dimension estimations of the scrambled picture consumes a semi-irregular conduct.

***Index Terms*: DNA sequences, SHA-256, PWLCM.**

I. INTRODUCTION

The image security problem can be solved efficiently and accurately using techniques like Bit-plane shuffling, DNA sequences for image encryption provide confidentiality and authenticity using SHA-256(Secure Hash Algorithm) and XOR of matrices using PWLCM method.



Due to the non-periodicity and affectability to the underlying quality, riotous guide is by all accounts a device that can be utilized for picture encryption. An algorithm for triple image based on chaotic sequences with Deoxyribonucleic acid (DNA) rules and its operations with excellent performance. Firstly, SHA256 hash value of combinational plain images one behind other and 16 bits were taken and are utilized to create introductory estimations of framework parameters of tumultuous frameworks for perplexity and use DNA rules for diffusion process. Then, each 8 bit planes of the three basic images remain knotted built on sequences generated by logistic map. After that each image is segmented into 8 blocks then sequences generated by lts,tss,lss order of these sequences are determined, based on this DNA rules are selected for each block of image. Then, image is shuffled using sine and tent maps. For DNA decoded image bitwise xor operations are done with random image generated by pwlcm. Test results and security examination validate that the calculation has belongings of enormous key space, tall affectability to important, solid opposing to measurable and differential assault.

II. RELATED WORK:

With advancement of networked multimedia techniques and internet, provides a way to send image information over various communication channels [1]. To protect that image information from illegal copying and distribution is big challenge today and challenges are increasing day by day from hackers. By using image encryption algorithms, the sender encrypts the plaintext into the cryptograph script. Just the approved beneficiary could unscramble the figure content with the mystery key(s) to acquire the plaintext. With rapid development in technology high data rates can be achieved, but now the problem is to send it in secured manner. This makes to follow the procedure of complex parallel data processing at higher speeds[7,8]. Turbulent frameworks have productive qualities, for example, high affectability to beginning conditions and framework parameters, ergodicity, blending, etc, confusion based picture encryption calculations are recommended increasingly secure and quick encryption techniques which take after wanted cryptographic properties.

Tumult based picture encryption calculations can be ordered into three kinds: perplexity, dispersion strategy and aggravating structure. The disarray calculations just scramble the places of the plain-picture pixels.

Histograms of together basic-image and cryptograph-image remain same since pixel values are constant. There are many methods to describe permutation algorithms and can be iterated many times.

Revised Manuscript Received on June 14, 2019

Y.S.V.Raman, Department OF Electronics & Communication Engg, Lakireddy Balireddy College Of Engineering, Mylavaram, Andhra Pradesh, India..

A.Narendra Babu, Department OF Electronics & Communication Engg, Lakireddy Balireddy College Of Engineering, Mylavaram, Andhra Pradesh, India.

The diffusion algorithm provides a way to change pixel values of plain image. Recent studies suggest that bit plane decomposition method is one of excellent method in diffusion process which is presented here. So, diffusion procedure is must to make it more secure. For all the picture encryption calculations, the figure picture ought to be shifted extraordinarily from its unique structure. Of this variation container be slow in two ways: NPCR and UACI. NPCR alludes to amount of pixels alteration degree while one-pixel of the basic picture remains altered, and UACI alludes to bound together average changing force that estimates the normal power of contrasts between the plain picture and the figure picture [2,3]. More encryption rounds can attain better encryption consequence, yet more adjusts would devour additional time that had been not utilized in this calculation so as to accomplish tasteful outcomes.

III. TRIPLE IMAGE ENCRYPTION

Many picture encryption calculations were proposed dependent on 1D or 2D tumultuous maps/frameworks. The 1D chaotic system have a nature of simplicity in structure and are easy of implementation, in any case, they also have a few imperfections, for example, little key space and powerless security. For improvisation in the security of these encryption algorithms, the higher dimensional systems were used. Be that as it may, the high dimensional frameworks are unpredictable in their structures and various parameters were utilized which increment in the expense of equipment/programming usage and the calculation multifaceted nature [4,5]. Be that as it may, numerous turmoil based picture encryption calculations are not verify enough, which can be split by means of certain assaults, for example, picked number gratified attack, realized simple content assault and selected basic gratified attack.

The new 1D riotous framework was produced after the Logistic, Tent and Sine charts. The new 1D tumultuous framework must bigger confused range and preferred turbulent practices over those seed maps, which makes to utilize these appropriate maps for picture encryption in a superior manner.

Any Encryption calculation to be effective, the calculation should comprise of both disarray and dispersion. Here comes dispersion impact and couple of realities as pursues, for example, shading picture encryption dependent on DNA arrangement task, they changed three Hamming separations of the basic picture into decimal numbers. The picture encryption dependent on DNA subsequence activity and confused framework. Couple pictures encryption calculation uncovers the actualities. To recover the safety of the cryptosystem utilized the riotous framework to irritate the picture pixel locations and pixel esteems, besides after that achieved DNA trainings as indicated by quaternary cipher rubrics.

A. Logistic map

The Logistic guide is unique of renowned one dimensional confused maps. It is a basic dynamical condition by compound disorganized conduct. The scientific meaning container is communicated cutting-edge the accompanying condition:

$$Xn+1 = L(r,Xn) = rXn(1-Xn)$$

Where r remains a constraint by variety of (0, 4) and Xn represents yield muddled arrangement.

Toward watch his unquiet practices, its fork define and Lyapunov Exponent stay exhibited in Figs. 2(a) and 3(a). within the branching graph appeared in Fig. 2(a), noticed stroke demonstrates his nice misdemeanour and also the robust line speaks to its non-tumultuous property. Here stay 2 problems within the provision guide. to start out with, its disorderly vary is restricted. Indeed, even within this vary there area unit some parameters that create the provision guide to possess no turbulent practices. This can be confirmed through the clear zone in its junction graph and plot of the Lyapunov Exponent in Fig. 3(a). For the Lyapunov Exponent, a positive esteem implies a decent riotous property of a disordered guide. By way of appeared in Fig. 3(a), the Lyapunov Exponents of the provision guide area unit littler than zero once parameter r<3.57. Second, the statistics scope of the riotous arrangements is littler than (0,1), demonstrating the non-uniform circulation within the scope of (0,1). These restricted depressed the utilizations of the provision guide.

B. Tent map

The Tent guide is known for its tent-like shape in the chart of its bifurcation graph. It tends to be characterized by the accompanying condition:

$$Xn+1=T(u,Xn)=\{uXn2\} \qquad Xi<0.5$$

Its tumultuous property is appeared in bifurcation examination in Fig. 2(b) and Lyapunov Exponent investigation in Fig. 3(b). Both examination results demonstrate that its confused range is (2,4). The Tent guide has a similar issue as the Logistic guide: the constrained disordered range and non-uniform circulation of the variation thickness work.

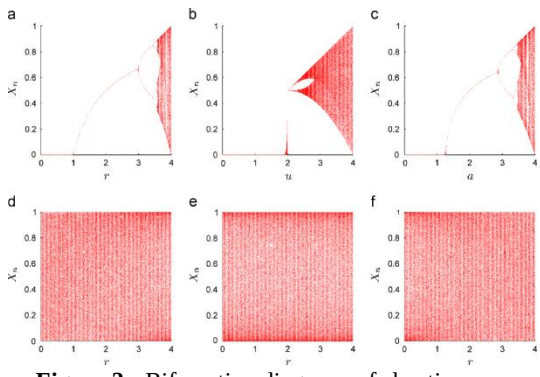


Figure 2 - Bifurcation diagrams of chaotic maps

C. The Logistic-Tent system

Up to presently we utilized the Calculated and Tent maps as seed maps. By and by the system utilizes the Logistic-Tent system (LTS). To improve its violent multifaceted nature, we connect the parameter settings for each seed outline, as characterized within the going with condition: Where parameter r (0, 4).

The bifurcation chart and Lyapunov Example of the LTS are showed up in Figs. 2(d) and 3(d), independently. Its wild run is inside (0,4), which could be a part greater than these of the Calculated or Tent maps. Its surrender groupings reliably pass on interior (0, 1) (see Fig. 2(d)). Thus, the LTS has way better disorganized.

D. The Logistic-Sine system

The Logistic-Sine system (shown as LSS) is the moment case of the proposed wild system. Its parameters are too bound together for simplicity.

$$Xn+1 = ALS(r,Xn) = (L(r,Xn)+ S((4-r),Xn)) \bmod 1= rXn(1-Xn) + (4-r) \sin(Xn)/4 \bmod 1$$

where Figs. 2(e) and 3(e) appear its bifurcation chart and Lyapunov Example comes about. The chaotic behaviors of the LSS exist within the entire run of parameter settings and its chaotic arrangements have a uniform-distribution inside (0,1).

E. The Tent-Sine system

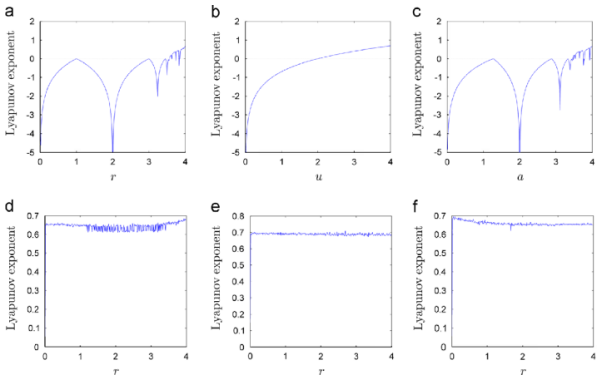


Figure 3 – Lyapunov exponent diagrams of chaotic maps

Utilizing the Tent and Sine maps as seed maps, the proposed tumultuous system in Eq. turns into another tumultuous system called the Tent-Sine system (TSS). Its definition can be portrayed in Eq. within the wake of bringing together its parameter settings.

$$Xn+1 = ATS(r,Xn) = (T(r,Xn)+ S((4-r),Xn)) \bmod 1$$

where constraint r (0,4). As appeared in Figs. 2(f) and 3(f), the TSS has astounding tumultuous possessions comparable by the LTS and LSS.

Arnold's Cat Map:

In this procedure, the comprehensive 2D Arnold's cat map, as well-defined by [6], remains recycled in execution the variations.

$$Xnew\ Ynew = 1\ a\ b\ 1+ab\ XY \bmod M$$

where $a, b \in \{1, 2, \ldots, M-1\}$, is the square medium size, $x, y \in \{1, 2, \ldots, M\}$ signify the pixel column and row locations popular the image correspondingly and xnew , ynew stretch the new column and row positions for the pixel under revolution, correspondingly.

On behalf of a grid T of scope M × M, the summed up 2D Arnold's feline guide ought to be iterated M2 times. So as to contrast this technique and different strategies, a stage network is determined utilizing the opposite activity. It ought to be noticed that the yield esteems are increased by one to change the mod activity impact. For instance, so as to ascertain T11, let a = 2, b = 3, x = 1 and y = 1, at that point xnew = 3 + 1 = 4, ynew = 2 + 1 = 3 and T11 = 15.

Consequently, the permutation matrix T3 container be printed as

T3 = 15 2 5 12 6 9 16 3 13 4 7 10

The change impact on a 4 × 4 square dependent on the stage lattices. Despite the fact that they are extraordinary and may look proficient, the following area thinks about these systems for various network sizes utilizing a few insights and picture investigation criteria.

IV. DNA SEQUENCE ALGORITHM

The A DNA grouping contains four nucleic corrosive bases, i.e., adenine (A), cytosine (C), guanine (G), thymine (T). Twofold stranded DNA fulfills the standard of Watson-Crick correlative base matching: A sets with T, C sets with G, or An and T remain integral, and C and G are corresponding. In the parallel framework, 0 and 1 are correlative. Correspondingly, the paired numbers 00 and 11 are correlative, and 01 and 10 are likewise reciprocal. On the off chance that we utilize the four bases A, C, G and T to signify the parallel numbers 00, 01, 10 and 11, there are absolute 24 sorts of DNA coding plans. Be that as it may, among them just eight of them meet the Watson–Crick integral standard. for instance, the decimal digits "0123" (the relating double number is "00011011") can be encoded into one of them, for example, "CTAG", "CATG", "GTAC", "GATC", "TCGA", "TGCA", "ACGT" or "AGCT".

In the event that we utilize the four nucleic corrosive bases C, T, An and G, to signify the double estimation of 00, 01, 10 and 11 individually, every 8-bit pixel estimation of the gray scale picture container be encoded hooked on a nucleotide string, for instance, if the gray scale estimation of the pixel is 177, its paired esteem is "10110001", which can be communicated as the four 2-bit nucleotides "AGCT". In this paper, the DNA groupings are utilized to scramble the computerized pictures.

Every 8-bit pixel estimation of the gray scale picture can be encoded into a DNA arrangement with length 4 through utilizing A, C, T and G to speak to the paired qualities 00, 01, 10 and 11. For instance, if the grayscale estimation of the pixel is 121, its double esteem is "01111001".

Table 1

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

Table 2
The XOR operation for DNA sequences.

XOR	**A**	**C**	**G**	**T**
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Table 3
The addition operation for DNA sequences.

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

One can get the DNA arrangement "CTGC" by the DNA encoding rule. On the other hand, the first twofold arrangement can be acquired by a similar standard, though utilizing diverse DNA deciphering guidelines will prompt unmistakable parallel groupings, e.g., another paired succession "00101100" is gotten by utilizing the DNA translating rule 3 to unravel a similar DNA arrangement "CTGC".

So as to encourage the utilization of DNA figuring in cryptography, some natural and mathematical activities are presented for the DNA successions, for example, expansion (+), subtraction (-), selective or (XOR) tasks, etc. In our project, the XOR, correlative then expansion tasks for DNA arrangements are utilized to scramble and decode the advanced pictures. The XOR, corresponding and expansion tasks for DNA arrangements are performed by the customary XOR, reversal and expansion in the double, separately. Comparing to eight sorts of DNA encoding rules, there are additionally eight sorts of DNA XOR principles, and eight sorts of DNA option rules. Tables 1 and 2show the DNA

XOR besides expansion principles utilized in the projected encryption calculation, separately. After the tables, one can see that an improper in each line or section is one of a kind, to be specific, the consequence of the DNA XOR task or the DNA expansion activity is likewise extraordinary. The DNA XOR activity is automatic.

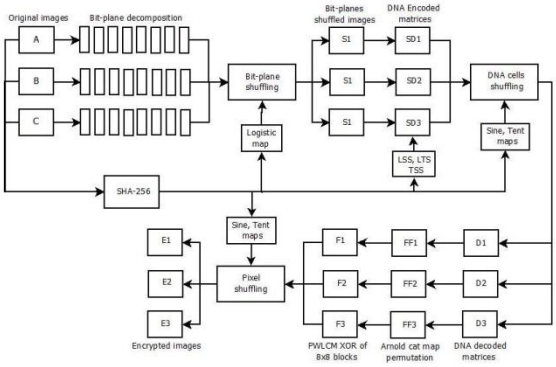
1. Compute the new limits and beginning circumstances by the mystery solutions and the first picture IO.

2. Decompose the plain-picture IO change the decimal grids into the paired frameworks with scope W×8H. At that point encrypt these double lattices by self-assertively choosing the DNA programming rubrics in Table 1, and get three DNA frameworks with scope W×4H. Now the irregular statistics ρ used to pick the DNA programming rules.

3. Compute the corresponding base of every component of the DNA network and play out the XOR task on the DNA grids and integral DNA framework

V. IMPLEMENTATION

Step-1:
Select three images, decompose them into bit Planes each and construct three images from them by shuffling bit-planes using Logistic map sequence. The Logistic map sequence is generated up to 24 values, these values are sorted. As there 24 bitplanes in total (8 bitplanes for each image) represented by sequence, the images are generated from each 8 bitplanes in each from sorted order.



Step-2:
Here we are using SHA-256 to generate 256-bit key steam based on the three grey level images are combined to form a3-dimensional image. Usually key steam is represented in hexadecimal.

Step-3:
Dividing the 256 bit key stream into 32 groups denoted by kl, kl},{l=1,2…..32},then the sum of 32 groups is computed using equation sum= ∑kl.

Step-4:
The parameters for the LSS, LTS, and TSS arecomputed using formulas:
3 parameters can be found by
r(i)=mod((bitxor(k(3*i-2),k(3*i-1))+ k(3*i) + sum)/(2^8),1)/5 +3

The next three parameters are found by
r(i)=mod((bitxor(k(3*i-2),k(3*i-1))+ k(3*i) + sum)/(2^8),4)/5
Where k(i) represent ith group of key.
By observing, both the values are adjusted to range between 3 and 4, since chaotic show effective behaviour in that range.

Step 5:
The 8 initial values are generated using formula as given below, which are used in LTS,LSS,TSS.
for i<6,
u(i)=mod((bitxor(k(38-6*i),k(36-6*i))+k(34-6*i) + sum)/(2^8),1)
and for i=7,8
u(i)=mod((bitxor(k(6*i-35),k(6*i-33)) + k(6*i-31) + sum)/(2^8),1)
Where k represents ith group of key.

Step 6:
Segment the each image into 8 parts and applyb8 DNA rules (as described in theory part) randomly By LSS, LTS, TSS sequences on the segmented Parts using parameter and initial values which are obtained from step 3, 4.

Step7:
Shuffle the pixels among the images using sine and tent map sequences using parameter and initial values which are obtained from step 3, 4 and decode DNA matrices by any of DNA rule.

Step 8:
Permute the images using Arnold cat map permutation technique[7].

Step 9:
Generate 8x8 random matrices using PWLCM sequences and XOR these matrices with the 8x8 segments of the images continuously by placing the result in respective segment and XOR that segment with next segment.

VI. CONCLUSION

A This paper proposed for triple images based on chaotic sequences with Deoxyribonulcie acid (DNA) rules and its operations with excellent performance. Firstly, SHA256 hash value of combination plain images one behind other, 16 bits were taken and is used to make first standards of scheme constraints of disordered systems for misperception and to use DNA rules for diffusion process. Then, each 8 bit planes of the three basic images are knotted founded on sequences generated logistic by map. After that each image is segmented into 8 blocks then sequences generated by lts, tss, lss,order of these sequences are determined, basing on these DNA rules are selected for each block of image. Then, image is shuffled using sine and tent map. The DNA decoded image is bitwise xor operations with random image generated by pwlcm. Of those experiments carried out for analysis of security includes key sensitivity, histogram analysis, auto correlation, fighting difference bout analysis, entropy and timing study. Furthermore, performance analysis showed that this approach of algorithm is safe and applied request of safe message.

REFERENCES

1. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci 273:329–351
2. Chai, X., 2015. An image encryption algorithm based on bit level Brownian motion and new chaotic systems. Multimedia Tools and Applications, pp.1-17.
3. Zhou, S., Wang, B., Zheng, X. and Zhou, C., 2016. An Image Encryption Scheme Based on DNA Computing and Cellular Automata. Discrete Dynamics in Nature and Society, 2016.
4. Liu, H. and Wang, X., 2013. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. Journal of Systems and Software, 86(3), pp.826-834.
5. Dixit, A., Dhruve, P. and Bhagwan, D., 2012. Image encryption using permutation And rotational xor technique. Natarajan Meghanathan, et al.(Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT, 6, pp.01-09.
6. Abd-El-Hafiz, S.K., AbdElHaleem, S.H. and Radwan, A.G., 2016, June. Permutation techniques based on discrete chaos and their utilization in image encryption. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2016 13th International Conference on (pp. 1-6). IEEE.
7. Wang, X. and Xu, D., 2014. A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dynamics, 75(1-2), pp.345-353.
8. Ashok Kumar P.M., Vaidehi V, "A Transfer Learning Framework for Traffic Video using Neuro-Fuzzy approach", Sadhana, Indian academy of science, Springer, vol 42, issue 9, pp: 1431-1442, Sept 2017.
9. Ashok Kumar P.M., Vaidehi V, " Detection of Abnormal Temporal Patterns from Traffic Video Sequences Consisting of Interval Based Spatial Events", KSII Transactions on Internet and Information Systems, vol 9, issue 1, pp:169-189, jan 2015

Data mining, Machine learning. He executed several Projects from DST, SERB

AUTHORS PROFILE

Y.S.V.Raman obtained his B.Tech, M.Tech and Ph.d in ECE from Andhra University and JNTUK. He authored more than 30 articles in reputed journals, conferences. His main research interests include Speech processing,

A.Narendra Babu obtained his B.Tech, M.Tech and Ph.d in ECE from SV University. He authored more than 30 articles in reputed journals, conferences. His main research interests include Speech processing,