# +A Novel Chaotic Map Encryption Methodology for Image Cryptography and Secret Communication with Steganography

**Jafar A. Alzubi, Omar A. Alzubi, G. Suseendran, D. Akila**

***Abstract--- Image steganography based on various methods like LSB method of hiding data image to cover images are most common method for secret communication. There are many steg-analysis algorithms available for to detect hidden data in an image. There are many existing cryptography methods for image encryption like DES, AES, RSA, etc. but these are of less security on attack.In order to overcome these above mentioned drawbacks a novel chaotic map algorithm has been introduced for image encryption and further proceeded with PPM (Pixel Pattern Mapping) algorithm for image hiding. The algorithm computes chaotic encryption method on RGB planes of the image to be hidden then is followed by PPM based image hiding method on cover image. Our method includes RGB image for encryption instead of gray scale image as in state-of-art methods.***

***Keywords--- Novel Chaotic Map Encryption, PPM-based-Steganography, Asymmetric Encryption Method.***

## I. INTRODUCTION

Image capturing has been carried out without contact to the object is the commonly used technology of remote sensing. A large amount of data will be in picture format pictures. However, it's is difficult to protect the data and to assure the security after modification of type, size.Image secret writing method will be helpful in secret communication with confidentiality assurance of the secret content there are many secret image encoding algorithms used as in[12-13].

There are two types of secret writing concepts one is secret writing in spatial domain [3-6]and other on networking domain[8-9]. This secret communication can encode an image with data. This data may be text, audio,video,binaryetc which can be encoded or hidden to an image or video which can be communicated over any transmitter or any channel.

The idea of image programmingexploitation is thechaos to that the some of ability of the dynamic machines is to produce one by one number format that is in sequence that square the measure in nature as random number. All messages are squared measured encrypted for exploitation sequences. As well foremost distinction among chaos and cryptography coding uses a key, but chaos having some initial parameters, appreciate the key. There are 2 square measuring stages in all image cryptosystem using chaos those are diffusion and confusion. In the confusion stage is wherever elements square measure permutated haphazardly specified they're disorganized everywhere the image with none. Disturbance with the pixel values, exploitation varied random key generated and chaotic mappings are occurred. Thus , images had been created already as unrecognizable, for the usinginitial constraints and management arguments serving because of personal key.Though I t is not a terribly immune to stolen and broken simple. So that we tend to go for diffusion stage.

In this method of Diffusion, the excited element are unit changed later on with varied functions as well XOR programming. These Confusion, diffusion methods knows the information that is firmly encrypted format, with breaking the attacks. The ides of hyper chaos theory is introduced in the reference[6] and differentiate about the mappings of low level and high level chaotic mappings. thus this theory says the virus of selected cipher crime and therefore the issues of restricted key. This is based on the concept of people in the pre-defined programs and houses of lower level chaotic process.

Reference[14] having a new chaotic coding methodology been projected with the permutation as in bit-level for the use of scrambling the dimensions within the stage of confusion. Including a pseudo-random generator for chaotic process, that having non-linear and give the sturdy bits with long orbits. It ends up with multiplied levels in security with assurance for the coding. Piecewise linear chaotic map is introduced in reference[15] with presenting the bit-level permutation mistreatment. As well one chaotic machine having song loopholes that may be resolved by joining the 2 chaotic roots and generating new algorithms.The function of XOR matrix for disseminating with the values and combining supplying makes an attempt to identical in reference [16]. Will increase key house similarly because the cipher attacks will have anti-attack power. For those all the histograms and entropy levels that is encrypted pictures are unit onerous to interrupt and area unit chaotic maps as in initial conditions those are combined having sensitive unit area.

**Revised Manuscript Received on May 15, 2019.**

**Dr. Jafar A. Alzubi,** Associate Professor, School of Engineering, Al-Balqa Applied University, Salt – Jordan. (e-mail: j.zubi@bau.edu.jo)

**Dr. Omar A. Alzubi,** Associate Professor, Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Salt – Jordan. (e-mail: o.zubi@bau.edu.jo)

**Dr.G.Suseendran,** Assistant Professor, Department of Information Technology, School of Computing Sciences,Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.
(e-mail: suseendar_1234@yahoo.co.in)

**Dr.D. Akila,** Associate Professor, Department of information Technology, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.
(e-mail: akiindia@yahoo.com)

Steganography based on Least significant Bit is widely used and most simple stenographic technique of data hiding in spatial method where secret image is hidden in lease significant bit ofcover image[1], [2].Pixels are selected in random way which makes difficult to identify pixels location.

Chaotic map encryption algorithms are highly complex to be detected. This method can be used to select secret pixel sequence in binary and gray images. Chaotic map method includes various techniques as initial process of encryption like logistic and tent map, Logistic and singer map, Logistic and sine map, Logistic and chebysev map.

This chaotic map methodis very robust and highly secure from hidden data detection. Due to these advantages they have wide range of application in the field of secret communication.

It has been observed that cover image carrying secret information is highly secure to detection by steganalysis. Use of a supporting image and chaotic map method gives a highly secure LSB image steganography method. This chaotic map encryption method is highly complex that includes multiple steps in an iterative method. Iteration for unpredictable times improves complexity method for deciding the position for secret pixel sequence and to create a random sequence that is highly robust which will be embedded to secret pixel sequence in cover image, we use a novel chaotic map encryption algorithm in order to encrypt the secret image, where alteration of the cover image is eliminated but contains 50% of the secret information.The image encrypted and cover image are of same size which enhances the robustness to hidden data detection.

## II. RELATED WORKS

*IN the year of 2007"Algorithm that is AES which is modified for encryption of image "has been published*

The paper was on analysis of advanced concepts in cryptography like in the technique is a key stream generator has been added to AES performancefor improvement of complete of the cryptography and improved Encryption standard (AES),

*In the year of 2008"Image Encryption Using Block-Based Transformation Algorithm, was published by Aman, Mohammed Ali*

Authors introduced a new method for combing image transformation [22] by usinf block based transformation method and this method was an advancement of Blowfish algorithm.System follows the procedure as follows block division, rearrangement, rework, encryption as in blowfish algorithm rule. This method increased the quantity of blocks resulted in considerably faded performance

*In the year of 2008,"Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm"was published by Debasish, BibhudendraAcharya and Saroj Kumar Panigrahy*

In [23] self-invertible matrices are created for Hill cipher algorithm. The mistreatment key has been to encrypt gray images over color images. This system designed ina way that works for all kinds of gray scale image. But has an exemption of photographs with similar background, or same color or gray level..

*An Image Encryption Approach by permutation and combination Approach Proposed by Encryption"AmanJantan, Mohammed Ali in the year of 2008.*

In [24] a combination method for image encryption that combines permutation of images was presented. Images are divided to 4x4 blocks and permutation method has been used for creating cipher out of it. Finally encrypted image has been obtained by the above algorithm. Thus results showed some better performance compared to above methods also helped to achieve better entrophy.

*Image Encryption Methodology Using Dynamic Hill Cipher Algorithm was proposed, by Sarat Kumar Patra, Saroj Kumar Panigrahy, BibhudendraAcharya in the year 2009.*

This paper invented a complicated hill method for encryption methodology. For secret encoding an involuntary key matrix has been used as cipher rule.They encrypted original imagewith different algorithms and used AdvHill cipher method. The encryption degrades the performance of the system when images are of identical colour or gray level. And this system works for all kind of images gray scale or colour.

*In 2011 by using majority logic criterion statistical analysis of S-box in image encryption applications are developed*

Tariq Shah, IqtadarHussain, Muhammad AsifGondal and HasanMahmood[28] proposed a paper to investigateS-boxes prevailing and study ofstrengths as well weaknesses and to see the correctness in cryptography of image software. The decided criteria use the result from correlation, distinction, correlation, and energy and this mean of absolute deviation. Ther=se are applied in advance cryptanalysis in affine-power-affine(APA), SKIPJACk, S8, AES, and XyiSboxes.

*In 2011, proposals on image security using Genetic Algorithm.*

RasulEnayatifar and AbdulHananAbdullah[27] projected atechnique support a new model using a geneticrule and a chaotic performed for the image cryptography. In the technique it support a hybrid model that consists a replacement algorithmic rule and perform for image cryptography. In that technique, firstencrypted photos unit of measurement created exploitation the initial image with the help of the chaotic perform. inside succeeding stage, these encrypted photos unit of measurement used as a result of initial population to starting the operation ofgenetic formula. Then, thatformula is utilized to optimizeencrypted photos the most quantity as potential. In the end, the foremost effective cipher-image is chosed as a result of the ultimate cryptography image.


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

*Image coding victimization Affine remodel andXOR Operation, 2011*

JyotiPrakash Singh, Amitava Nag, Srabani Khan, SaswatiGhosh, SushantaBiswas, D. Sarkar and ParthaPratimSarkar[26] propose a a try of section committal to writing and secret writing algorithms that's supported shufflingimage pixels victimization affine remodeling that they encrypting the subsequent image victimization XOR operation. They distribute the half values to altogether whole totally different location victimization affine remodel technique with 4 8-bit keys. The reworked image then divided into a strive of pixels x a strive of pixels blocks and every block is encrypted victimization XOR operation by four 8-bit keys. Their results tried that after the affine remodel the correlation between half values was considerably attenuated. And the key size utilized in rule is sixty four bit[31][32].

## III. PROPOSED SYSTEM METHODOLOGY

A novel Chaotic map encryption system has been introduced in this paper. Chaos theory has been used for generating this method. The method involves unpredictable encryption of images with moment becomes random. In chaotic system an exponential increase in uncertainty in very forecast manner. There are many chaos system introduced [17] some are as follows

*Singer map*

This singer map system performs singer iteration method. And in chaotic system it is as stated below

$$S_{n+1} = \mu(7.86 * S_n - 23.31 * {S_n}^2 - 28.75$$

μis between [0.9, 1.08].

The chaotic statistic square measure $S_n \in [0, 1]$.

*Logistic map*

Logistic map isintriguing map which is too simple and the mapping is done by the following equation.

$$x_{n+1} = r * x_n(1 - x_n)$$

Where $x_n$ =the population of the ordinal generation

r= is that the rate of growth, conjointly referred to as bifurcation issue. This map gives wide variation in the growth rate depending on the initial condition.$x_n \in [0, 1]$ and management parameter r ϵ [3.569946, 4] and n ϵ N.

*Piecewise map*

Piecewise map has been represented by four distinct partitions as stated in below equation

$$P_{n+1} = \begin{cases} \frac{P_n}{a}; 0 \le P_n < a \\ \frac{P_n - a}{0.5 - a}; a \le P_n < 0.5 \\ \frac{1 - P_n - a}{0.5 - a}; 0.5 \le P_n < 1 - a \\ \frac{1 - P_n}{a}; 1 - a \le P_n < 1 \end{cases}$$

Where d = endpoints of 4 subintervalsϵ [0, 0.5]. However, the chaotic sequence generated lies in the interval$P_n \in [0, 1]$.

*Chebyshev map*

Chebyshev map is explained by the following iteration function:

C_(n+1)=cos⁡(n* 〖cos〗 ^(-1) C_n)

wherever n is that the iteration vary. Victimization this map, chaotic data point ϵ [0, 1] unit of measurement obtained.

*Tent map*

Tent map [11] is one in each of the foremost studied and wide used chaotic maps that are accustomed generate pseudo-random numbers in many applications, like secure cryptography. it's printedas follows:$T_{n+1} = \begin{cases} \frac{T_n}{\mu}; 0 \le T_n < \mu \\ \frac{1 - T_n}{\mu}; 1 - \mu < T_n \le 1 \end{cases}$

wherever μ is that the management parameter and once μ ϵ (0.4, 0.5) and $T_0 \in [0, 1]$, for all n≥1 the generated series $T_n \in [0, 1]$ tends to be in a very comparatively ideal chaotic state.

*Sine map*

The pure mathematics circular function map is based on the circular function iteration function and it's printed as follows:

x_(n+1)=a*sin(π*x_n)

wherever0≤ a ≤1whereas the data point of sort x_n ϵ [0, 1]. For a=1, unit of measurement generated by this map .that generates series tends to be chaos, whereas for different values of a, the series might or won't be in chaos.

This paper it to use the different chaotic indications to urge private key. By using the diffusion and confusion the security is enhances by notion of chaotic maps at intervals of the improved cryptography. By using the block cipher chaos based image cryptography is applied.In the instance of 128, 256, 512 bits each length for instance for the every cipher generated by the blockcipher. The steps for coding and cryptography are as follows:the generated secret key is countermined into mounted lengthfor the decryption/encryption fro the initial and as well output cipher.

The unit of measurement for the cryptography followed in the two phases:

Phase 1: secret key generation.

Phase 2: image cryptography.

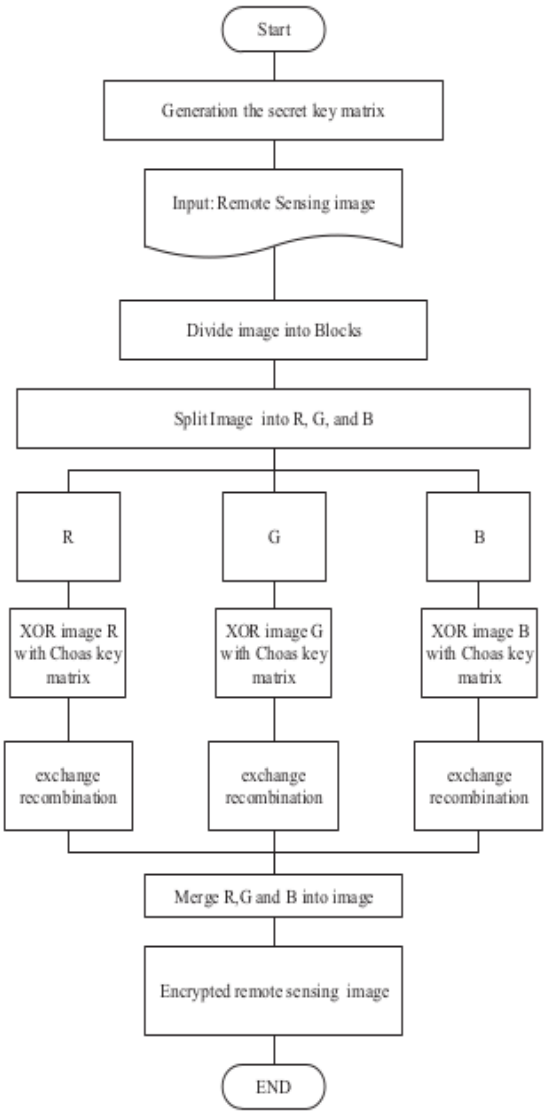
*Secret key generation (Chaotic system)*

The condition for the one of the ought encrypted info is to the key.and this is deemed for extra vital to the formulafor secret writing as a result of so many reasons, if the key isn't acknowledged first, encrypted data will be keep in as unknown, and the second is, because of the brute-force crime the key space is need to be safeguard in significantly large and the third,if the secrecy ofkey is not effective. thenkey written data unit is broken. [11].

Inherently,secret key isn't addicted to the plaintext, hence, whole completely different keys area unit is use to inscribe the different cipher-text which is a plain-text. As the result, the processes is impractical which give the shortage of a correct key [10].

In a methodology ofsecret writing key encompasses an important role as a result of dearth of a secrecy key will suggeststhe cipher image that will be acknowledged by hackers. The key space needed is to be sufficient sizeable to make sure safeguarding from all style of hackers by Consequently,[11]2 advocates a decent secret writing formula. That is to be prone to the cipher keys,randomness is created through chaos speculation because of brute force attacks and safeguarding all styles of attacks.

*Image encoding and cryptography*




The next steps of algorithmic rule is illustrated below that the technique of image encryption. In a figure four the steps related to the key matrix the generation supported is illustrated.3 further the process is to image is splitted into blocks then the splitted image contains shuffling image contents like R, G, and B supported the secret key matrix. And then, by using the chaos key matrix exchange XOR and recombination are applied to color R, G and B are supported by the three sub-images. Lastly, three footage are unified to original image.

Image encoding steps are as follows:

The opposite of cryptography, helps to rewrite the encrypted information by swinging the encrypted information back to their original file. This is supported by key matrix, the image which is shuffled the contents unit of measurement inversion back. Later , cipher image ar planning to 16x16 separated pixels as a non-overlapping blocks are as R, G, B and their sub images.XOR image are planning to the key matrix in the final the initial photos of three images are merged[33]. Following flow.

*Steganography with cowl image*

Pixel pattern matching is utilized for embedding the key information into the quilt image. during this algorithm, the info is embedded into the image whereas not changing the initial part price of the image. Here such pixels unit of measurement elite from the video whose price matches the information to be embedded. Moreover, the position of these pixels is noted. As throughout this system, the initial part price is not altered. As a result,there's no distortion due to the embedding of data [29]

Step1: select the quilt image ‘C’ from the video sequences, that had regenerate by victimization MATLAB code

Step2: Convert the image ‘C’ into unsigned variety format (uint8) and divide the quilt image into Red (R), inexperienced (G) and Blue (B) components

Step3: select the amount of input bits ‘n’ to be substituted in ‘C’

Step4: Now, do the logic AND operation to the amount of bits in R a part of ‘C’ and substituted ‘n’ bits

Step5: Then do the bit OR operation to the output of on prime of step and thus the whole shifted message bits with ‘n’ bits

Step6: Repeat a similar for inexperienced and blue components collectively

Step7: Do a similar methodology for all the chosen frames from the video file so convert R, G and B components into stego frame then once reconstruct all the frames into stego video, throughout that the message data has been embedded.

The system initial takes a secret message from the user. This substance is initially encrypted by creating use of the planned novel chaotic map formula. to supply a lot of security, this encrypted secret message is additional divided at intervals the vary of Quotient, Divisor and Remainder. The system presently asks the user for aimage file for embedding the information. once the user provides with a image, wherever the encrypted message at intervals the vary of Quotient, Divisor and Remainder is embedded victimization half Pattern Matching. as a results of the message is embedded, a location secret's generated for every half. This location secret's embedded in varied frames throughout a} terribly connected list fashion victimization LSB technique. once embedding the key message and so matters key, a stegoimage file is generated. This file is then shared with the individual receiver[34].

## IV. RESULT ANALYSIS

The algorithmic program projected was enforcedwith the employment of MATLAB language and MATLAB Tool. Security of the crypto system projected for photos as proofs and efficiency to the meanwhile of many experimental outcomes. Experiments and test were applied on the projected cryptography theme. The projected algorithmic program following the figures are the completion of the cryptography and their crypted images were simulated by experiments.


**Fig. 1: Data image to be hidden**

The cryptography steps square measure applied to appreciate the decrypted image, as are determined in Figs. 6. Cryptography needs Associate in Nursing economical cryptography rule the facility for endure the attack which is notable types. Those are differential attacks, mathematics and brute force[11-13].


**Fig. 2: Cipher image after chaotic encryption**

The histograms for original image Fig. seven and matching image with secret writing square measure typically discovered in Fig.8,9 and 10. As square measure typically discovered in this histogram, a part of values to the primary image area unit targeted on a positive values. this implies the contrawise of the bar graph which is distruction in the choices to the primary image of the secret writing.

In the meanwhile the figure four and five are demonstrates the bar graph of R,G, B components as well rather uniform and looks cipher image as a topresult and the frequency of information for the images is leak .The bar graph of the cipher image and the uniform significant measures that should be highlight at the cipher image.


**Fig. 3: Cover image for hiding cipher data**

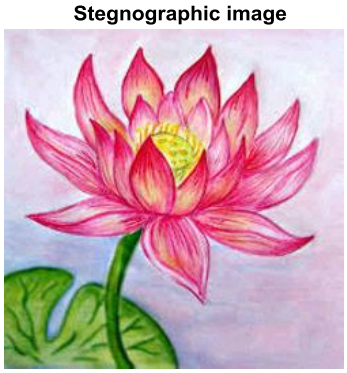



**Fig. 4: Image with Embedded Data**

The coding. The bar graph of cipher image's R, G, B components unit of measurement discovered whereas not increasing the image file size. After embedding the encrypted information image into the stego video Secret message of a significant amount characters is efficiently embedded into the video frames. the results achieved unit of mensuration on the far side the previous systems in terms of minimum distortion and a negligible increase in file size. as a results of the planned system build use of part pattern matching the distortion is negligible that we'll store a significant quantity of information into the frame Fig. 5and Fig. 6

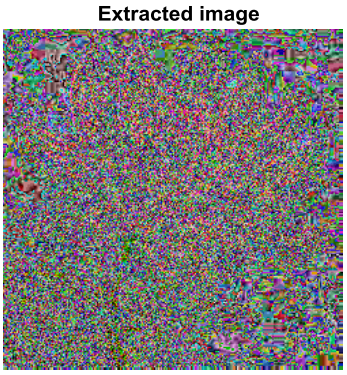



**Fig. 5: Cipher image extracted at reception side**


**Fig. 6: Decrypted cipher image**

The encrypted message severally. as a results of it's determined, there's not any noticeable variation between the 2 frames.Also, the placement secret is split and embedded into the numerous video frames apply coupled list fashion. owing to that the retrieval of the encrypteddata image become easy and quick at the receiver's finish.

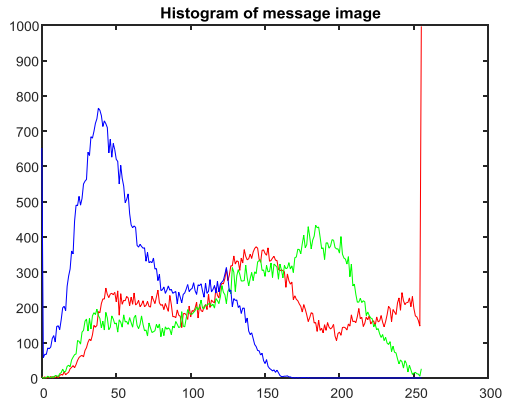



**Fig. 7: Histogram of message image**

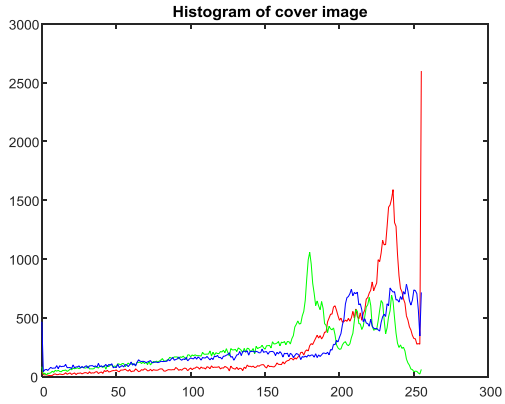



**Fig. 8: Histogram of cover image**

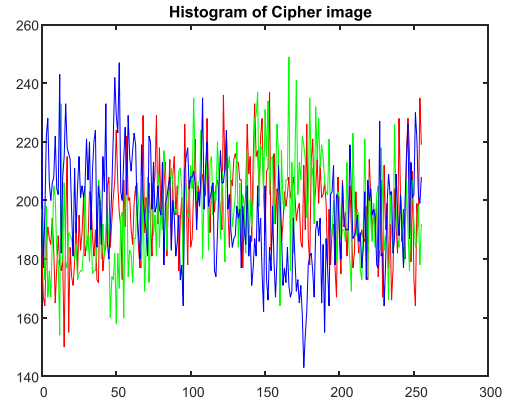



**Fig. 9: Histogram of cipher image**

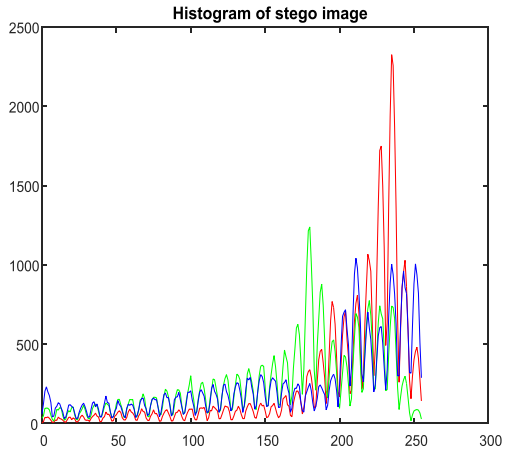



**Fig. 10: Histogram of stego image**

## V. CONCLUSION

A novel chaotic map image secret writing formula has been projected during this paper. As this projected formula is grounded on a completely unique chaotic map system, it'll solve the common issues associated with the formula is grounded in a chaotic map of low-dimentional.Thus on strengthen the security of a cryptosystem squre measure is applied to both pixel-level and bit level permutations. Many experiments are dead ina demonstration of a security and then responsibility in a projected formula of image secret writing.

Image security is also a endless downside and there should be the new techniques created aboard with increasing the varieties of cracks. during this paperthat we have a tendency to tend to mentioned and compared with the merged chaotic secret writing cryptographies that square measure accountable for bigger keys house and strong attack immunity. Among the varied combos enforced, provision and Tent map, signer map and logistic combination showed best results for varied take a glance at footage. Firstly, we have a tendency to tend to generated one dimensional sequence for every the chaotic map used which we have a tendency to born-again theninto second sub-chaotic arrays. The two sub-chaotic matrices square measure then combined to return up with Associate in Nursing secret writing matrix that's used to perform XOR operation with the initial pixel information matrix. Itprovides huge key house and may be used even for encrypting extraordinarily classified footage transmission in fields like military and medicine. The technique will helps to effectively hiding the images from the attackers, has howling ability to to deal with cipher attacks, it is ability to cipher attacks.

## REFERENCES

[1] W. Luo, F. Huang, and J. Huang, “Edge adaptive imagesteganography based on LSB matching revisited”, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, 2010.

[2] J. Melad, and Saeed, “A new technique based on chaotic steganography and encryption text in DCT domain for color image”, Journal of Engineering Science and Technology, 2013, vol. 8, no. 5, pp-508-520.

[3] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, Yu. Hai, Information Sciences 181 (6) (2011) 1171.

[4] N.K. Pareek, PatidarVinod, K.K. Sud, Image and Vision Computing 24 (9) (2006) 926.

[5] TiegangGao, Zengqiang Chen, Physics Letters A 372 (4) (2008) 394

[6] Qiang Zhang, Ling Guo, Xiaopeng Wei, Mathematical and Computer Modelling 52 (11–12) (2010) 2028.

[7] Zhengjun Liu, Xu. Lie, Ting Liu, Hang Chen, Pengfei Li, Shutian Liu, Optics Communications 284 (1) (2011) 123.

[8] Nanrun Zhou, Yixian Wang, Lihua Gong, Hong He, Wu. Jianhua, Optics Communications 284 (12) (2011) 2789.

[9] Yu Zhu, Zhe Zhou, Haibing Yang, The 2nd IEEE International Conference on Advanced Computer Control, IEEE Computer Society, Shenyang, 2010, p. 217

[10] Sankpal PR, Vijaya PA. Image encryption using chaotic maps: a survey. InSignal and Image Processing (ICSIP), 2014 Fifth International Conference on 2014 Jan 8 (pp. 102-107). IEEE.

[11] Ephin M, Joy JA, Vasanthi NA. Survey of Chaos based Image encryption and decryption techniques. InAmrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA) 2013.
[12] Akhavan, A. Samsudin, A. Akhshani, "Cryptanalysis of an image encryption algorithm based on DNA encoding", Optics & Laser Technology, vol. 95, pp.94-99, 2017.
[13] X. Zhang, X. Wang "Multiple-image encryption algorithm based on mixed image element and chaos", Computers & Electrical Engineering, vol. 62, pp. 401-413, 2017
[14] S. E. Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.
[15] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.
[16] W. Wang, M. Si, Y. Pang, P. Ran, H. Wang, X. Jiang, Y. Liu, J. Wu, W. Wu, N. Chilamkurti, and G. Jeon, "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.
[17] Fister, M. Perc, S. M. Kamal, and I. Fister, "A review of chaos-based firefly algorithms: Perspectives and research challenges," *Applied Mathematics and Computation*, vol. 252, pp. 155–165, 2015.
[18] Radwan, A. G., &Abd-El-Hafiz, S. K. (2013). Image encryption using generalized tent map. *2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS)*. doi:10.1109/icecs.2013.6815499
[19] Tomida, A. G. (2008). Matlab Toolbox and GUI for Analyzing One-Dimensional Chaotic Maps. *2008 International Conference on Computational Sciences and Its Applications*. doi:10.1109/iccsa.2008.7
[20] Y. Wu, J. P. Noonan, S. Agaian, "NPCR and UACI randomness tests for image encryption." Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) (2011): 31-38. Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018) IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1978-1-
[21] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.
[22] Mohammad Ali BaniYounes and AmanJantan ―ImageEncryption Using Block-Based Transformation Algorithm‖IAENG International Journal of Computer Science, 35,2008.
[23] Saroj Kumar Panigrahy, BibhudendraAcharya and DebasishJen‖, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm‖1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008
[24] Mohammad Ali BaniYounes and AmanJantan, ―An ImageEncryption Approach Using a Combination of Permutation Technique Followed by Encryption‖, IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.
[25] BibhudendraAcharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,‖ Image Encryption Using Advanced Hill Cipher Algorithm‖, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
[26] Amitava Nag, JyotiPrakash Singh, Srabani Khan, SaswatiGhosh, SushantaBiswas, D. SarkarParthaPratimSarkar, ―Image Encryption Using Affine Transform and XOR Operation‖,International Conference on Signal Processing, Communication, Computing and Networking Technologies ICSCCN 2011).
[27] RasulEnayatifar , Abdul Hanan Abdullah, ―Image Security via Genetic Algorithm‖, 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.
[28] Tariq Shah, IqtadarHussain, Muhammad AsifGondal , HasanMahmood,‖ Statistical analysis of S-box in image encryption applications based on majority logic criterion‖, International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011
[29] S. Bhat, M.Wagchaude, A. Wadnekar, T. P. Nagarhalli, "Enhanced Steganography Using Pixel Pattern Matching", IEEE Int. Conference on Engineering and Technology(ICETECH), March 2016
[30] Ms. Fameela. K. A, Mrs. Najiya. A and Mrs. Reshma. V. K, "Survey on Reversible Data Hiding in Encrypted Images", International Journal of Science, Engineering and Technology
[31] J. A. Alzubi, O. A. Alzubi, and T. M. Chen, A Forward Error Correction Based On Algebraic-Geometric Theory, 1st ed. Springer International Publishing, (2014).
[32] J. A. Alzubi, O. A. Alzubi, and T. M. Chen, A Forward Error Correction Based On Algebraic-Geometric Theory, 1st ed. Springer International Publishing, (2014).
[33] S.Suganya, S.Padmaja, G.Suseendran "MRI Geometric Distortion for Brain Tumor Detection and Segmentation**",** Journal of Advanced Researchin Dynamical and Control Systems,Vol. 9, No. 7, August 2017 pp-77-82
[34] T.Nathiya, G.Suseendran, "An Effective Way of Cloud Intrusion Detection System Using Decision tree, Support Vector Machine and Naïve Bayes Algorithm", International Journal of Recent Technology and Engineering, Vol.7(4S2), 2018 pp.38-42.