Review Article

A Comparative Study on Image Encryption Techniques

Hitesh Kumar Chandak[1], Dr. Anshuj Jain[2]

[1]*M.Tech. Scholar, Department of Electronics & Communication Engineering, Scope College of Engineering, Bhopal (M.P.), INDIA*
[2]*Guide, Department of Electronics & Communication Engineering, Scope College of Engineering, Bhopal (M.P.), INDIA*

ABSTRACT

Picture Encryption or encoding of pictures is the techniques to safeguard picture being hacked or harmed while communicating. Such security strategy applied on communicates data starting with one hub then onto the next hub which is touchy to unveil and should be kept as secure as could really be expected. Past explores were having different security calculations to encode picture, and here this study examines the degree for enhancements in characterized boundaries of picture encryption to make encryption framework more dependable and heartier. In the proposed encryption algorithm security levels will conceivably partitioned in entire security framework in equal streams, which increases the heartiness of the relative multitude of layers (RGB). A definitive objective of the algorithm is to accelerate the encryption and decoding process.

KEYWORDS

Chaotic Map, Matrix Operations, Cipher Image, Fast Encryption, elliptic curve encryption, encryption de-encryption, image encryption

1. INTRODUCTION

Encryption is the study of concealing data which can be uncovered exclusively by real clients. It is utilized to guarantee the mystery of the sent information over an unstable channel and forestall snooping and information altering. Another field called cryptanalysis. Worries with going after and unscrambling these codes. Numerous Encryption plans were proposed and utilized for getting information, some utilization the common key Encryption, while some others utilize the public key Encryption (PKE). The common key Encryption is a framework which involves just a single key by both source and beneficiary to scramble and unscrambling messages. Then again, public key Encryption utilizes two keys, to be specific private-key and public-key. To encode a message in the public key plan, the public-key is utilized, while the private-key is utilized to decode it.

When contrasted with the common key Encryption, the public key Encryption is somewhat sluggish. Nonetheless, the public-key Encryption can be utilized with the common key Encryption to bamboozle both. Specifically, the public key Encryption enjoys numerous upper hands over the common key; among others, it expands the security and comfort where disseminating the private key to other party isn't needed.

Elliptic bends are arithmetical bends which have been read up by numerous mathematicians for quite a while. In 1985 independently proposed the public key cryptosystems utilizing elliptic bend. From that point forward, numerous specialists have gone through years concentrating on the strength of ECC and further developing procedures for its execution. The Elliptic bend cryptosystem (ECC) gives a more modest and quicker open key cryptosystem. Likewise, the ECC is additionally a practical and tied down innovation to be carried out in obliged applications, like the RFID.

Producing bends to function as Encryption bends should go through various calculations and methodology in order to make a solid Encryption bend. An elliptic bend over a limited field Fq, where q = pm, is really particular on the off chance that p separates t, where t is the hint of bend. Notwithstanding, ANSI X9.63 (ANSIX9.62 1999) states that a bend is supposed to be really particular provided that E (Fp)=p+1. The created bend should not be defenseless against referred to assaults like Menezes, Okamoto, and Vanstone assault (MOV), as they showed how the Elliptic Curve Discrete Logarithm Problem (ECDLP) could be diminished to the Discrete Logarithm Problem (DLP) in the augmentation field of This assault is effective on an extremely unique class of bends known as really solitary bends or MOV. Nonetheless, this assault can be tried not to by chip away at the field sizes north of 113 pieces. For this situation, decreasing the bend won't surpass the base acknowledged field size.

The ECC has been financially acknowledged, and took on by many normalizing bodies, for example, American National Standards Institute ANSI, Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). ANSI in their standard gives the required calculations to produce

an elliptic bend and creating Elliptic Curve Digital Signature (ECDSA) marks. It gives bit by bit guides to create and confirm ECDSA to separate key sizes.

Elliptic bends characterized over limited fields which give a gathering structure used to carry out the Encryption plans. Scalar point duplication is a significant structure square of all elliptic bend cryptosystems, an activity of the structure $k \cdot P$, where k is a positive number and P is a point on the elliptic bend. Working out $k \cdot P$ gives the aftereffect of adding the direct P toward itself for the specific k-multiple times, which brings about one more point Q on the elliptic bend. The backwards activity, for example to recuperate k when the focuses P and Q = $k \cdot P$ are given is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP). No sub remarkable time calculation has been known to address the ECDLP in an appropriately chosen elliptic bend bunch. The picture encryption offers two significant advantages over the RSA; it has greater security per bit and a reasonable key size for equipment and current correspondence. As needs be, this outcome in more modest public key endorsements, lower power prerequisites and more modest equipment processors.

To build the security and utilize the biometric highlights by creating private keys and delivering Elliptic Curve space boundaries, this postulation joined the elliptic bend and biometric elements to solidify the seed that will be utilized to produce the bend against the cryptanalysis. The planned framework involves iris signature as information to help creating the expected Elliptic Curve boundaries. The produced boundaries will be utilized in the Encryption cycle like Elliptic Curve Digital Signature Algorithm (ECDSA).

Encryption depends on hard numerical issues like indivisible number factorization, Elliptic bend discrete logarithm issue and discrete logarithm issue. The thought behind these issues is the calculation can be effectively done in one course, yet it is truly challenging the other way. It is easy to track down the consequence of duplicating two numbers, yet observing prime elements of a number is very difficult. Consequently, Encryption is worried about the plan and the examination of numerical methods which can offer secure correspondences within the sight of pernicious enemies. It is a region which is worried about the change of information for security reason.

2. CHAOTIC MAP

The chaotic behavior is one of the possible behaviors of a nonlinear system, which apparently looks random for specific values of system parameters. The phenomenon of chaos theory was first introduced by Edward Lorenz in 1972 with conceptualization of "Butterfly Effect". The important characteristics of chaos are its extreme sensitivity to initial conditions of the system. It is purely resulting from the defining deterministic processes. Small differences in initial conditions yield widely diverging outcomes for such dynamical systems, making long-term prediction impossible in general. The theory was summarized by Edward Lorenz as "Chaos: When the present determines the future, but the approximate present does not approximately determine the future."

Everything frameworks can be comprehensively delegated deterministic, stochastic (probabilistic) or chaotic map of which chaotic map are generally erratic. Chaotic map guides are in many cases utilized in the investigation of dynamical system which show conduct that is exceptionally delicate to introductory circumstances and, surprisingly, little annoyances can yield generally separating results. Still these systems are deterministic in light of the fact that in view of the underlying condition future way of behaving can be anticipated, subsequently, their way of behaving could be called as deterministic chaos.

The essential standard of chaos based encryption is to utilize the dynamical system to create an arrangement of numbers that are pseudo-irregular in nature and these successions could be utilized as a key to scramble input picture. For given boundaries two beginning circumstances can digress dramatically into two distinct directions. These boundaries can be utilized for encryption and decoding and keys can be browsed these circumstances. Due, to these chaos boundaries and introductory condition we could create an enormous key space which further upgrades the security. On account of the irregular way of behaving, the result appears to be arbitrary to the aggressor while just the source and collector realize that the system is clear cut.

Chaotic qualities are valuable in producing keys, hash capacities, computerized marks and so on which are helpful in cryptography. Utilization of confusion has made the encryption interaction similarly quicker in light of simplicity to produce long tumultuous pseudorandom arrangements whose values is by all accounts uncorrelated assuming that underlying worth and related boundaries for age of succession are not known yet security is a major concern and a proficient encryption strategy hearty to assaults stays a continuous test in research local area.

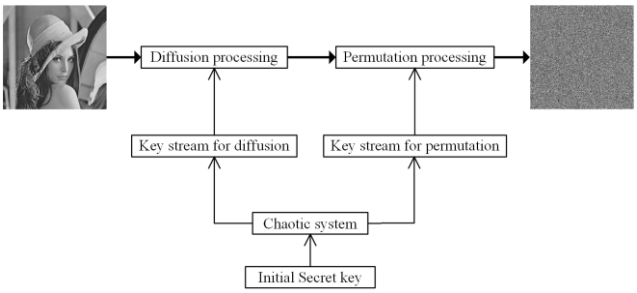

Fig. 1 Image encryption structure based on chaotic system

3. LITERATURE REVIEW

Sr. No.	Title	Author	Year	Approach
1.	"A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map"	Cengfei Chen, Kehui Sun, Qiaoyun Xu	2020	Color image is proposed with security at higher level. At First, simple to build with higher Spectral Entropy (SE) complexity 2-layered Cubic modulation map (2D-CIMM-ICMIC) has planned, which is very simple in form. Secondly, the initial values of 2D-CIMM map has been updated by using hash values of basic image in real time, by which the encryption algorithm sensitivity has increase to the plaintext and within fixed precision effect.
2.	"A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals"	Xuncai Zhang , Lingfei Wang, Zheng Zhou and Ying Niu	2019	In this approach a new image encryption technique is suggested where space filling characteristics of the Hilbert curve and the infinite characteristics of the H-geometric fractal is used. This combines the pseudo-randomness of hyper chaotic system and the sensitivity to initial values.
3.	"A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512"	Aqeel Ur Rehman , Huiwei Wang , Malik M. Ali Shahid , Salman Iqbal , Zahid Abbas , And Amnah Firdous	2019	A unique approach of discriminatory encryption for color images is suggested in which to change the primary conditions and controlling parameters of 1-Dimensional (1D) chaotic maps, SHA-512 hash of plain image has utilized. The red, green and blue channels of a color image are combined into 1D array and permute by using sorted index of a pseudo-random sequence.
4.	"Cryptanalysis and Enhancement of an Image Encryption Scheme Based on Bit-Plane Extraction and Multiple Chaotic Maps"	Yu Liu, Zheng Qin, and Jiahui Wu	2019	In this research multiple chaotic maps and bit-plane extraction-based security performance of image encryption is analyzed. Considering the identified security defects, logical know-plaintext and chosen original image threats are proposed for retrieving some data of the main plain image.
5.	"An Efficient Digital Image Encryption Using Pixel Shuffling and Substitution for Wireless Networks"	Islam T. Almalkawi, Jamal N. Al-Karaki, Ayoub Alsarhan, Randa, Deena Al-Mughrabi	2019	Here in this paper, chaotic algorithm based an efficient security system has designed to efficiently encrypt digital pictures over various applications of wireless network, considering the processing capacity and time compels of various wireless networks in account. In suggested algorithm the digital pictures processes in three stages as generation of security key, pixel permutation, and substitution.
6.	"A Chaos Based Image Encryption Scheme Using Digit-Level Permutation and Block Diffusion"	Ping Ping , Jinyang Fan, Yingchi Mao, Feng Xu, And Jerry Gao	2018	Propose a based on new digit-level has proposed. The Image pixel matrix has decomposed into three different digital matrices, and by using Henon map, these digital matrices are mixed up. The grade of pixel level permutation has been combined by the digit-level permutation with that of bit level permutation.
7.	"Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling"	Wei Feng and Yi-Gang He	2018	In this research, brief introduction about DS-HIES has discussed and figure out various security, practicability and realizable issues in it. Plaintext attack algorithm has chosen to crypt analyze the DS-HIES. Various relevant tests have been completed to confirm the precision of cryptanalysis and the suitability of the suggested algorithm.

8.	"Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy"	Chengqing Li, Dongdong Lin, Bingbing Feng, Jinhu Lü, and Feng Hao	2018	In This article Security deficiency of the chaos-based P-N sequence generator and the sensitivity mechanism has reported. Three basic parts of one round version of IEAIE can be divided with divide-and-conquer technique in differential attack scenario. Additionally, from the perspective of modern cryptanalysis; each and every used safety metric is questioned.
9.	"Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps"	Congxu Zhu and Kehui Sun	2018	RT-enhanced tent type chaotic map-based cryptanalysis color picture encryption scheme is proposed on this research paper. The cryptosystem's equivalent keys are successfully divided by using chosen-plaintext attacks and the target cipher text picture can be decoded

Cengfei Chen, Kehui Sun, Qiaoyun Xu [1]. In this approach, chaotic system-based encryption algorithm of color image is proposed with security at higher level. At First, simple to build with higher Spectral Entropy (SE) complexity 2-layered Cubic modulation map (2D-CIMM- ICMIC) has planned, which is very simple in form. Secondly, the initial values of 2D-CIMM map has been updated by using hash values of basic image in real time, by which the encryption algorithm sensitivity has increase to the plaintext and within fixed precision effect. Finally, bit level permutation and diffusion processes of the encryption algorithm are performed. In addition to this, simulation and performance analysis describes that the proposed algorithm has better security at higher level.

Xuncai Zhang, Lingfei Wang, Zheng Zhou and Ying Niu [2] In this approach a new image encryption technique is suggested where space filling characteristics of the Hilbert curve and the infinite characteristics of the H-geometric fractal is used. This combines the pseudo-randomness of hyper chaotic system and the sensitivity to initial values. At first, with the help of secure hash algorithm 3 (SHA-3) as the primary value of piece wise linear chaotic map (PWLCM) as well as Rossler chaotic system, hash value of a original image is calculated, which connects the key with original image. Additionally, the chaotic sequences which are created by chaotic systems are used to mix-up the global pixel positions and images pixel values, therefore disturbing the arrangement of the pixel positions and pixel values. Secondly, to disarrange the position of local pixel and dispersed pixel values two times, the Hilbert curve as well as H-fractal is used alternately.

Aqeel Ur Rehman, Huiwei Wang, Malik M. Ali Shahid, Salman Iqbal, Zahid Abbas, and Amnah Firdous [3] A unique approach of discriminatory encryption for color images is suggested in which to change the primary conditions and controlling parameters of 1-Dimensional (1D) chaotic maps, SHA-512 hash of plain image has utilized. The red, green and blue channels of a color image are combined into 1D array and permute by using sorted index of a pseudo-random sequence. The array of 1D permuted is dividing into three sub-arrays and then DNA encoding imposed chaotically on each pixel of every channel and then distinct every DNA encoded channel to their (LSB) and (MSB).

Yu Liu, Zheng Qin, and Jiahui Wu [4] In this research and multiple chaotic maps and bit-plane extraction-based security performance of image encryption is analyzed. Considering the identified security defects, logical know-plaintext and chosen original image threats are proposed for retrieving some data of the main plain image. Furthermore, the faults of IESBC has revised via multiple modifications as in diffusion stage, the statistical value of plain-picture is adopted; a relationship mechanism has built up between each location of the LSBs plane with the corresponding position in the MSBs plane to minimizing the interrelation among adjoining pixels of plain-image and random number source is utilized which makes IESBC compose a probabilistic algorithm and can oppose the plaintext attacks effectively.

Islam T. Almalkawi, Jamal N. Al-Karaki, Ayoub Alsarhan, Randa Abu-Ajamiyah, Deena Al-Mughrabi [5] Here in this paper, chaotic algorithm based an efficient security system has designed to efficiently encrypt digital pictures over various applications of wireless network, considering the processing capacity and time compels of various wireless networks in account. In suggested algorithm the digital pictures processes in three stages as generation of security key, pixel permutation, and substitution. Here in encryption process, 256-bit long security key is being used. In the substitution and permutation stage, 2D Logistic chaotic map is utilized for image pixel transfer and transposition, in order to enhance the needed security level and resist against various security threats.

Ping Ping, Jinyang Fan, Yingchi Mao, Feng Xu, and Jerry Gao [6] In This method permutation based on new digit-level has proposed. The Image pixel matrix has decomposed into three different digital matrices, and by using Henon map, these digital matrices are mixed up. The grade of pixel level permutation has been combined by the digit-level permutation with that of bit level permutation. At first it is proposed that a digit level permutation takes digit as its compact processing segment. The pixel matrix of the ordinary image is decomposed into three different matrices at the digit-level in the time of permutation. Then using Henon map, every matrix is disarranging for three separate rounds with different controlling parameters. Finally, a shifted image is gotten by the three scrambled matrices which are reassembling into a new pixel matrix. After permutation this method can change the circle graph of the simple image, and this is more efficient than the bit-level permutation.

Wei Feng and Yi-Gang He [7] In this research, brief introduction about DS-HIES has discussed and figure out various security, practicability and realizable issues in it. Plaintext attack algorithm has chosen to crypt analyze the DS-HIES. Various relevant tests have been completed to confirm the precision of cryptanalysis and the suitability of the suggested algorithm. The results of test has shown that various security issues are pointed out do exist in it, the proposed chosen plaintext attack algorithm is feasible for it and one can completely recover the basic image without knowing the information related to secure key.

Chengqing Li, Dongdong Lin, Bingbing Feng, Jinhu Lü, and Feng Hao [8] In This article Security deficiency of the chaos based P-N sequence generator and the sensitivity mechanism has reported. Three basic parts of one round version of IEAIE can be divided with divide-and-conquer technique in differential attack scenario. Additionally from the perspective of modern cryptanalysis, each and every used safety metric is questioned. Furthermore, every used security metric is capable to taste real security performance. To design a productive and safe media encryption scheme, the various related critical factors, e.g. the special characteristics of multimedia data, the concrete application scenario with specified constraints, and computation load, should be considered completely.

Congxu Zhu and Kehui Sun [9] RT-enhanced tent type chaotic map based cryptanalysis color picture encryption scheme is proposed on this research paper. The cryptosystem's equivalent keys are successfully divided by using chosen-plaintext attacks and the target cipher text picture can be decoded. An improved encryption algorithm is suggested based upon the cryptanalysis. Another logistic-tent map is applied to the better encryption algorithm, and specification of the plaintext picture connected with the SHA-3 hash value is presented as a mystery key parameter so that the enhanced algorithm can oppose chosen-plaintext threats. The safety analysis and trial tests results that improved algorithm can significantly increases the security of encrypted images and all the merits of the basic algorithm are still possessing.

4. PROBLEM DESCRIPTION

The image encryption applications produce their private keys utilizing a got irregular key generator. What's more, it additionally utilizes a haphazardly created seed to deliver the bend space boundaries. This produces arbitrary number where cryptanalysts might take advantage of it. This additionally makes the need to have an elective method for making the seed utilized in delivering the private key and the bend space boundaries trouble to procure or fake it. Rather than the arbitrary generator, iris mark is utilized to deliver the expected seed as an elective way, which is utilized to create the private keys and the space boundaries. The created bend is interesting, considering the way that the Iris highlights are remarkable. This uniqueness of iris can give a higher security regarding the trouble of procuring the iris mark of a person without his endorsement of snapping a photo of his eye.

5. CONCLUSION

The growing for more and more secure systems has led researchers worldwide to discover and implement newer ways of encryption. Public key Encryption techniques are gaining worldwide popularity for their ease and better strength. With the rapid developments of the communication and applications of multimedia techniques in recent years lead the researchers to focuses on the security of digital data over the internet. In this paper we have discussed the use of Elliptical Curve Encryption for ciphering color images. The work will be done to achieve benefits and security parameters.

REFERENCES

[1] Cengfei Chen, Kehui Sun*, Qiaoyun Xu, "A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map" in Electrical, Electronics, China Communications, May 2020 pp.12-20.

[2] Zahir Muhammed, Ziad Muhammad and Fatpih Özkaynak, "Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique" IEEE Access, vol.7, pp.99945_99951, 2019.doi10.1109/ACCESS.2019.2930606.

[3] Nazir A. Loan, Shabir A. Parah, Javaid A. Sheikh, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption" IEEE Access, vol. 6, pp.19876_19897,2018. doi 0.1109/ACCESS.2018.2808172.

[4] Sudeshna Bora, Pritam Sen and Chittaranjan Pradhan, "Novel Color Image Encryption Technique using Blowfish and Cross Chaos Map" IEEE ICCSP 2015 conference.pp.0880-0883.

[5] Congxu Zhu and Kehui Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps" IEEE Access, vol. 6, pp. 18759_18770, 2018. doi 10.1109/ACCESS.2018.2817600.

[6] Chengqing Li, Dongdong Lin, Bingbing Feng, Jinhu Lü and Feng Ha, "Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy" IEEE Access, vol. 6, pp.75834_75842,2018. doi 0.1109/ACCESS.2018.2883690.

[7] Wei Feng and Yi-Gang He "Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling" IEEE Photon. J., vol. 10, no. 6, Dec. 2018, Art. no. 7909215.

[8] Yu Liu, Zheng Qin and Jiahui Wu "Cryptanalysis and Enhancement of an Image Encryption Scheme Based on Bit-Plane Extraction and Multiple Chaotic Maps" IEEE Access, vol.7, pp. 74070_74080, 2019. doi 0.1109/ACCESS.2019.2916600.

[9] Wang Xingyuan and Zhao Hongyu "Cracking and Improvement of an Image Encryption Algorithm Based on Bit-Level Permutation and Chaotic System" IEEE Access, vol.7, pp. 112836_112847, 2019. doi 0.1109/ACCESS.2019.2935017.

[10] Hossam Diab "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations" IEEE Access, vol.6, pp. 42227_42244, 2018. doi 109/ACCESS.2018.2858839

[11] Ping Ping, Jinyang Fan, Yingchi Mao, Feng Xu, and Jerry Gao "A Chaos Based Image Encryption Scheme Using Digit-Level Permutation and Block Diffusion" IEEE Access, vol.6, pp. 67581_67593, 2018. doi 0.1109/ACCESS.2018.2879565

[12] Sinha, A., & Singh, K. (2003). "A technique for image encryption using digital signature" Optics communications, 218(4), 229-234.

[13] Panchal, D., Jani, C., & Panchal H., "An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing." International Journal of

Engineering Development and Research. Vol. 3. No. 4 IJEDR, 2015.

[14] Kumar, S., Sinha, B., & Pradhan, C. (2015). "Comparative Analysis of Color Image Encryption Using 2D Chaotic Maps. In Information Systems Design and Intelligent Applications" (pp. 379-387). Springer India.

[15] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," Nonlinear Dyn., vol. 84, no. 4, pp. 2333_2356, 2016.

[16] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," Opt. Lasers Eng., vol. 77, pp. 118_125, Feb. 2016.

[17] Y. Liu, X.-J. Tong, and J. Ma, "Image encryption algorithm based on hyper chaotic system and dynamic S-box," Multimedia Tools Appl., vol. 75, no. 13, pp. 7739_7759, 2015.

[18] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Opt. Lasers Eng., vol. 78, pp. 17_25, Mar. 2016.