ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse731022021.pdf
https://doi.org/10.30534/ijatcse/2021/731022021

Approaches of Chaotic Image Encryption models in Enlightening Image Storage and Security systems

Pradheep Manisekaran[1]*, Prachi Dhankhar[2], and Parveen Kumar[3]
[1]Department of Computer Science and Engineering, NIMS University Rajasthan, Jaipur-303121, India.
Email: Pradheep45@hotmail.com
[2]Department of Computer Science and Engineering, NIMS University Rajasthan, Jaipur-303121, India.
Email id: Prachi.sirsa@gmail.com
[3]Department of Computer Science and Engineering, NIMS University Rajasthan, Jaipur-303121, India.
Email id: pk223475@gmail.com

ABSTRACT
The present life scenario has become completely digital and intelligent in all aspects, including the way of communication, production methodologies, medical sciences and other entertainment domains. Out of all domains, communication plays a vital role in every human life and the same is valid for corporates who handle bulk amount of data to be transmitted. This may include a multimedia data transfer between defense authorities of various countries or between a commercial information sharing centers. Under these circumstances, such information is to be transmitted in a secured channel. Unfortunately, secured fiber optic or any other wired communication is highly expensive and not affordable for infinite number of users. Hence, most of the communications among people are only through wireless channels. Due to the tremendous developments in communication standards up to 5G, people prefer wireless communications to cover the whole part of the world. As the information is freely available to anyone in the form of electromagnetic waves, it is impossible to share privately through a common wireless network due to week encryption methodologies. Simultaneously key space is not abundant. This has been highly inspired to pursue research in a different direction to a greater degree and to develop the measurements of current cryptography protocols and procedures. Choosing a chaotic encryption domain has several compelling explanations as described here.
Keywords: Chaotic systems, Space-Time diagrams, KS entropy density, bifurcation diagram, Space-Amplitude diagram.

I. INTRODUCTION

In the present trending life, people are always surrounded by challenges. Since network-based communication has been introduced, anyone connected to the network could hack the system and access the data. Just because hacking threat is common, it is not possible to stop communication. It is essential to develop some concepts such as cryptography in order to establish communication even in the region of challengers. The issue is related to encryption, key allocation and decryption. The current cryptographic world uses scientific approaches to ensure that every data and multimedia user follows the recommended methods with a better conviction.

Present social media, such as Facebook, WhatsApp, Instagram etc., have increased the data traffic and utilize the maximum bandwidth of the channels. Hence these data transfer requires a trustable media to share the information.

The statement is applicable not only to the high end defense, flight and ship control communication but also to the common men's communication. Figure 1.1 shows the basic architecture of encryption and decryption algorithm.

To accept an encryption method as a compromising one, there are certain requirements to be verified on it. Commonly expected methods are visual check, key length, key sensitivity analysis and security limits. In addition to this, images generated through diverse technologies such as X-ray, CT (Computer tomography) scan, ultra sound which is used in medical diagnosis and medical healings should maintain their respectability as the nature of images is responsible for human lives. Confidential storing of images without communication inside a server in premises too is a challenging task as hackers are many and may emerge from anywhere. Figure 1.2 shows a simple version of Chaotic based image encryption technique.

It is seen that the plain text image undergoes confusion and diffusion and finally altered as cipher image. Confusion is done for N-Rounds and overall image alteration is done for M-Rounds. This iterative modification of the original image is the major strength of the chaotic image encryption [1].

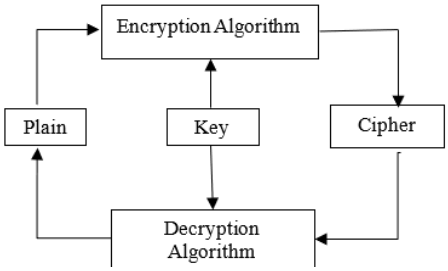


Figure 1.1 Block Diagram for Encryption and Decryption

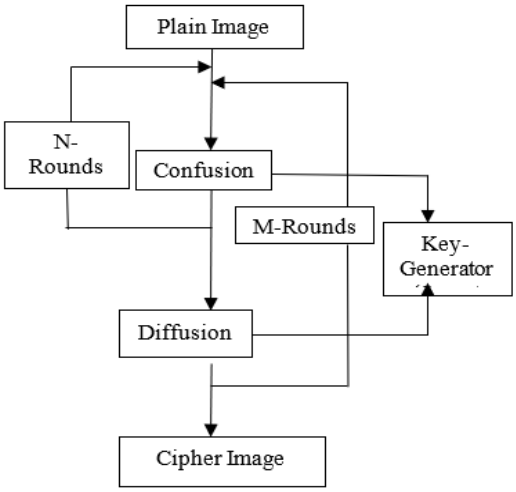


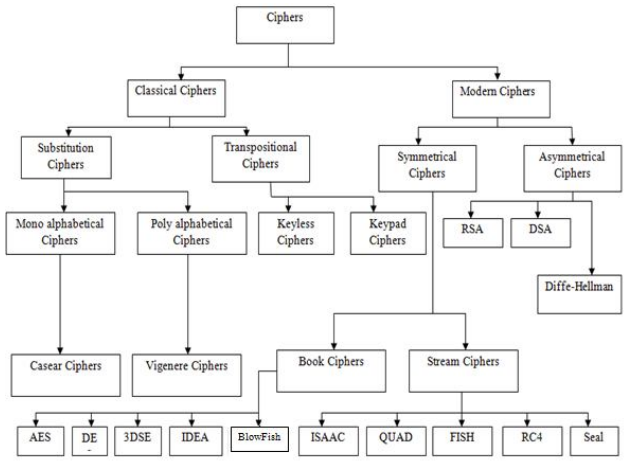
Figure1.2 Schematic of chaotic image encryption technique

Security systems basically work towards implementing cryptography, watermarking and steganography. Cryptography is treating the whole image as valid content and changing the appearance of the image and transmitting it. Water marking is to hide a text or image inside an image transmitting it. This is highly useful in copyright protection as well to transmit images in a secured manner. Steganography is almost similar to watermarking except that extracting the original host image is not a major constraint and only the text or image hidden is considered worth. As time passes, cryptographic algorithms have emerged from its basic architecture to tremendous developments based on the increase in the hacking intelligence. Various types have been shown in Fig. 1.3

More number of users on internet opens an easy way and tempts to misuse the data available in cyber space. This is basically because of huge business potential involved in the internet-based commercials. Every piece of information is valuable in internet media. Hence hackers are someway motivated and forced to misuse the data and make money out of it. So, stopping every internet hacker from performing crime is very difficult task and it is done by the way the data is kept protected in data storage as well as in transmission [3].

When the matter of image comes into consideration, there are two things to be done. (a) Adopting encryption procedures at end to end and (b) some methods to protect the copy rights of the image and any legal cross verification, which has been named as watermarking technique. Steganography is for some different applications which is used to communicate text data via an image or an audio stream. Media security as a whole is a system described by set of equations or techniques to protect the content. Standard symmetric key cryptography is sufficient to protect the correspondence of digital images and any other text based media. Such an encoding scheme could be realized using cryptosystems such as Advanced Encryption System (AES) or Data Encryption system (DES).

Figure1.3 Various Cryptographic Algorithms



It is to be seen whether the media is a continuous stream or standard binary data, based on which the encryption procedures could vary. Various encryption transforms available are Affine transform, Arnold map, Tangram algorithm, Baker's transformationand Magic 3D square transformation. However, these methods could not withstand for surprise attacks tried by hackers [2].

1.1 Terminologies in image encryption

- **Plain text**

The original image or text to be communicated is usually called as plain text.

- **Cipher text**

The encrypted content is named as cipher text and it would be very difficult to understand the content and usually in a non-readable format.

- **Encryption and Decryption**

A process in which a plain image is converted into cipher image using an encryption algorithm and key is called as encryption. Encryption is done at the transmitter side and decryption is done at the receiver side who is assumed to be an intended user. Decryption is the method of transferring incomprehensible encrypted message to plain text.

- **Key**

Key is known to both transmitter and receiver and it might be a numeric integer or alpha numeric text or binary.

The following targets are met while using cryptography.

- **Confidentiality**

Information is not known to anyone except transmitter and receiver.

- **Authenticity**

Not only the information, but also the transmitter and receiver identity is verified through cryptography.

- **Integrity**

Through cryptography an alteration in data could also be detected.

- **Non denial**

Overall cryptography ensures that both sender and receiver should not be able to deny the transmission.

There are three different types of domains in which encryption is done namely; Spatial, frequency and hybrid domains. The following content presents the various works related to aforementioned encryption domains.

1.2 Terminologies in cryptography

Two broad categories are available as Symmetric and Asymmetric key encryption.

- **Symmetric cryptography**

Whenever the key is identical at both encryption / decryption sites, it is known as public key cryptography. The strength of this technique is its key, as protection lies primarily on the key. The corresponding methods are just some few examples of DES, TRIPLE DES, AES, RC4, BLOWFISH [3].

There are two types of symmetric algorithms, respectively block ciphers and stream ciphers [4].

- **Block Cipher**

Block cipher is a mechanism that maps 'n' bit simple text blocks into 'n' bit secret message text blocks; 'n' is called block length.

- **Stream Ciphers**

Stream encryption techniques are an important set of cryptography models. They encrypt single characters (usually binary digits) of plain text messages, one at a time, using a time-varying encryption method. Commonly, stream ciphers are faster than hardware block ciphers with fewer hardware circuitry. They are often much more appropriate and obligatory in some situations (e.g. in some telephone applications), where loading is limited or when scripts have to be stored separately when they are obtained. Leading to limited or no error propagation, stream ciphers can also be useful in situations where transmission errors are exceptionally high. possible. Stream ciphers are commonly classified as being synchronous or self-synchronizing.

- **Diffusion and Confusion**

Diffusion means that the frequency numbers of the letters in plain original text are spread over a number of characters in the encrypted message. Confusion means that the key is complexly linked to the encrypted message. In specific, each character of the original text should rely on a number of sections of the key.

- **Spatial Domain**

In the space domain process, every cryptography algorithm is implemented specifically on the pixels. If f(x,y) is a original text file, g(x,y) is a typically achieve image. One can point to the number of pixels on which the pattern cycles (its frequency) in the space domain.

- **Frequency Domain**

In this method of encryption, initially the original image is converted into its frequency domain by means appropriate transforms. Any alterations are done in frequency domain and converted into spatial domain through inverse transformations. In the same way, decryption is done in frequency domain and decrypted image is viewed after converting into spatial domain.

II. LITERATURE REVIEW

- **Chaotic Based Encryption**

A tool used by DCT, Huffman coding and Run Length Encoding (RLE) to execute compression and chaotic encoding are used. The correlation coefficient of the neighboring pixels in the longitudinal, perpendicular and diagonal directions are 0.0129,-0.0116 and 0.037 simultaneously for the encoded objects. It also results from a higher PSNR value between both the original image and the encrypted image, as can be seen from the corresponding various initiatives by the authors concerned.Moreover, vertical correlation coefficient is only 0.9533. Horizontal and Diagonal correlation coefficients are of 0.8978 and 0.8555 respectively. The key sensitivity has been analyzed for an original key of 0.1777 and modified key of 0.1778 whose decimal points are inadequate in recent unsecured communication channels [3]. Figure 2.1 displays the original and encrypted image obtained using their proposed method.

Figure 2.1 Original and Encrypted image

It is transparent that many researchers have focused their attention towards chaotic based encryption schemes. Works done previously also introduces a lossless compression along with a better encryption scheme using bit permutations. Number of pixels change rate (NPCR) and Unified Average Change in Intensity (UACI) has been obtained as 99.63% and 33.42% in their experiments. The major strength of the paper claimed was its key space of 2140 which is insufficient for present day encryption systems [4].

Although disorderly encryption-based systems have been studied, several benchmarks have also been analyzed to assess the transferability of the encryption scheme in order to obtain the best results. Centralized image encryption and compression will always promise an exchange between limitations including such key space, PSNR, CR, UACI, NPCR, coefficient of correlation and histogram distributions, etc. The biggest downside in earlier literature was relevant to both chaotic and non-chaotic encryption, with only key space, PSNR and correlation coefficients illustrated. In comparison, earlier studies only concerned with the encryption method, but not the study of the unpredictable behavior of the system. However, the problems domains of key space, mutual information among the lattice keys, improvement of NPCR and UACI needs to be improved. In addition, the quality of the reconstructed images has been analyzed only with conventional PSNR metric. It is suggested that, some more metrics such as Figure of Merit (FOM) which is already used in image compression can be vitally used further.

- **Spatial Domain**

Robert and Matthews found that chaotic system properties and its output is very sensitive to the initial conditions. Moreover, pseudo random outputs are very difficult to guess the original content after some number of iterations [15].

Tent map has been used as a chaotic map where the original plain text image is iteratively modified to haze the intruders. Statistical attacks were performed on the cipher image by Chi square test. It was found that the number of iterations greater than 73 and key length to be 20 gives satisfactory results [16].

Schwartz proposed a shuffling method to encrypt an image. A seed is initially generated and it is used as a key. Using this seed, random number generator is activated and those random points are grouped. By using a line drawing method, the plain image is consequently encrypted [17].

Kuo used an encryption method where the phase spectrum of the original image is used as an alternate to the conventional key. Since the phase information is dynamically changed, the resultant cipher image is unrecognizable [18].

A Chang and Liu have integrated compression and encryption where the file is first compressed using Quad tree and then encrypted using SCAN. Quadtree is a lossless encoding, but the overall form may not be immune to stabbing, such as jigsaw riddle attack and neighbor assault, and so on[40]. Alexopoulos et al, suggested a way of encrypting 2D grayscale images using a fractal class[19].

Yet another method proposed was the most compromising method to implement encryption using holographic 3D process. Those researchers could demonstrate this successful method by using original image and a reference image helping as an encryption key. This method was highly useful in local authentication systems [20].

It is found that PerPermutation was found to have been used in large parts such the plain image material was permuted to get the encrypted image. 2D maps were used to create modern symmetric block encryption schemes [44]. This scheme is especially useful for the encryption of significant data measurements, such as digital files. Baptista suggested a hunt for disorderly block ciphers [21].

Mutation has been used in huge pieces so plain image content were permuted to get encrypted image. Two dimensional maps had been used to make a new symmetric block encryption schemes [44]. This scheme is particularly valuable for encryption of substantial measure of data, such as digital images. Baptista proposed a searching based chaotic block ciphers [21].

A low computational complexity was achieved by Guo and Yen while reaching a task of high security. They have introduced and used an effective mirror like encryption algorithm for images using a peculiar chaotic system [5]. Further extension was done where VLSI architecture was proposed. Initially a chaotic sequence was generated and based on the sequence; gray levels of the pixel were 'Xor'ed or 'Xnor'ed done as bitwise operation [6]. Almost similar work was done where a different chaotic map was used. Lorenz attractor based mathematical expression was realized for image encryption. The extension was implemented in FPGA board for various images [7].

The main aim of chaotic based encryption is to scatter the data which could result in hazing the intruder. To reach these chaotic properties such as Lyapunov exponents and ergodicity, they should be maintained as positive quantity. Not all the chaotic systems are highly secured. Some weak chaotic systems appear to be with strong encryption, but they are easily breakable and valuable information of "how encryption is done" is available to attackers. In order to protect images due to this problem, Masuda and Aihara used discretized tent map to eliminate this problem to some possible extent. So, properties of such attractive chaotic systems have been proposed by utilizing the dynamical qualities. [8]

Few forms of physical layer codes for wireless and wired networking networks have also been proposed [9]. The original image signature is applied to the encoded vector of the original image. BCH codes are being used for this intention both at the sender and at the receiver level. Thus, the dignity of the image is protected by certain strong coding techniques.

While observing the research work carried out by this team, it is seen that Baker's map had been used to improve the existing symmetric key algorithm which originally fits only for square images [22]. But this work supports a variable size image and an additional strength was proposed by Sallen et al. In the research work done by Shin et al, multilevel encryption had been proposed. A gray-level image was divided into several binary images composed of the same gray-level images. Furthermore, binary images were stored in binary phases with binary random process images. The total encrypted image was achieved by combining all the encoded binary images of the wise layer[23].

Author also suggested that 1D chaotic map was used where keys were from various sources such as beginning state and number of iterations [24]. Wang Ying et al, used both permutation and a non-linear chaotic map to discourage the hackers. The basic problem in this work was its periodicity, which allows the intruders to guess the image data [25].

Many researcheswork shows the periodicity analysis after they had done scrambling in their image. They used a T-matrix and found the period is twice the length of Arnold matrix [26]. The work was found suitable for image watermarking tasks. Neural networks have been used in addition to the existing chaotic systems and the system has been named as chaotic neural system [27].

In order to improve the pseudorandom properties of chaotic sequences, permutation and cross sampling works has been attempted and executed [28]. Two chaotic systems are used where one to produce chaotic sequence which in turn transformed into a binary value by using a threshold function and the other chaotic system is used to permute the image matrix [29].

Stream cipher approach has also been used in few papers where a multi chaotic system was preferred. Pixel Chaotic Shuffle (PCS) and Bit Chaotic Rearrangement (BCR) methods were introduced in their works. In PCS stage, the color image pixel locations are shuffled using Henon, Chua, Rossler and Lorenz maps. Further stage was to change the values of pixels whose range of values were normalized in the range of 0 to 1. Because of this, the key space of 10180 has been obtained. This method could eliminate the exhaustive attack [30].

In research work carried out by Musheer et al., 3 diverse chaotic maps were used. The color image was first partitioned into number of blocks based on the size of the image. These blocks were shuffled using Cat map. Further distribution of blocks was done where the final shuffled pixels were obtained. Final encryption was done using 1D logistic map. The key space obtained through this method was 10112 and found very sensitive to even a smallest change in the key. The correlation was extremely as low as 0.0095. This lower value reveals that the visual appearance of the encrypted image was completely different from the original image. An entropy value of 7.9992 was obtained which indicates that there exists only a minor data loss [31]. It uses four-dimensional hyper anarchy as a valid extension. Three sequences are used for the three layers R, G and B, and the fourth sequence is used for the final encryption. It is correct that the correlation coefficients of the encoded picture are substantially diminished and it is also worth noting that a minor improvement in the hidden key has culminated in a completely reshaped and varied image[32].

It is interesting to refer literatures where PWLCM (Piece-Wise Linear Chaotic Map) was used. This map has been found as an appropriate method for the design of encryption systems. Initially, the color

image is transformed into three layers and then transformed into its phase space using tent map. This phase space is divided into 256 sub intervals. The key space achieved is 1093. This quantity is comparatively a small key space size. An actual benefit of this work is its robustness against the animal power assault. High values of NPCR and UACI are obtained along with an entropy is 7.9551 [12].

- **Frequency Domain**

As mentioned earlier, encryptions done in frequency domain has also attracted the research people. 3D jigsaw transforms where the images were first transformed into bit planes and each plane was separated into more small blocks. Fractional Fourier Transform (FRFT) was used to encode the image [33].

Almost similar work was done except that the transform used was fractional Mellin transform. The color images of its original color format of RGB into RGB supplement space. Shuffling of pixels was in 3D space. Vast key space obtained through this proposal could make the system highly robust [34].

A method was proposed that used Arnold transformation in the transform domain gyrator to encode color pictures. The color images were initially converted into R, G and B. The textures were initially encoded by adding random phase masks and transforming Arnold first phase and eventually transforming the gyrator. After this point, a second random phase mask and a second order Arnold transforms and transforms the gyrator. This process could send extra keys to the Arnold transformation in encryption and scrambling [35]. As a result, high protection was derived from severe risks of attack.

Orthogonal composite grating has also been used to encrypt data. As normal, the pictures were first divided into sections R, G and B and modified to an orthogonal composite grating. Twisted composite grating is then encrypted by two random phases of encoding. The study was believed to be very cost-effective by the corresponding authors [36].

Further, affine transform and gyrator transform has been utilized to perform a better encryption. The real and imaginary parts of the affine transform of the image were taken into account. Later R, G and B image qualities were scrambled using a random angle approach. As a last step, gyrator transform was applied to the result of the previous step. High security was claimed through this work [37].

In multimedia communication, whether it is static image or video, not all the portions of the information needed to be encrypted. In such Cases, performing encryption only on the parts of interest could save enormous time, cost and complexity in the algorithms. This could even reduce the design cost of the prototype when developed using VLSI techniques for real time applications. In order to attain the aforementioned tasks, they used an edge based lightweight image encryption plan [10]. Initially edges were detected based on the two-fold image in which presence of '1' is an edge pixel and '0' is non-edge pixel. By comparing the original and the detected image, blocks were estimated based on edge boundaries. Encryption is performed based on the significance obtained based on block comparison. 2D cross chaotic map and different order discrete fractional cosine transform were used for the purpose of encryption.

- **Spatial Domain**

There are some applications such as image recognition systems which are used in authentication systems. Commonly available authentication systems utilize the biometrics such as face, finger print, palm prints, iris etc, acquired from individuals. These systems acquire or scan the images in wider area. Not all the parts of the images need to be stored as it consumes storage space and contains redundant information in it. Prior to encrypt or compress the image, it is essential to segment the image and identify the significant portion of the image. A multi-level region of interest (ROI) based image encryption had been performed for a finger print biometric data. The key space obtained through their methods was 2128 [13]. Another advantage is its variability in encryption levels which could be adjusted based on the required recognition performance.

- **Hybrid Domain**

As the name of this subsection indicates, a combined method of both spatial and frequency is incorporated in proposed encryption algorithms are called as hybrid algorithms. The wavelet transforms and chaotic map has been combined to perform encryption. It is well known fact that wavelet transform divides the 2D image matrix into low frequency and high frequency bands. The significant information about the image is available in low frequency band [38]. The high frequency content of the image is 'XOR'ed with the scrambled low frequency band image content. After this, Arnold scrambling was performed on the resultant image. A key space of about 2128 was obtained with a total encryption time 0.266 s.

Major task was to ensure a good security over communication in public channels. Hence, researchers always make attempts to introduce a novelty which is an eternal process. Hybrid methods were of such type where both frequency and time domain methods are involved. Transformation and substitution stages were used to secure an image. Fourier transform and discrete wavelet transforms are used to convert time domain into frequency domain. Further tent map was used in transformation stage and Bernoulli's map was used in substitution stage [11].

III. PROBLEM STATEMENT

To present in its essence, the foremost challenge is to overcome the existing weak encryption methodologies. The following are the major challenges in this research area.

- Key space
- Methods to discourage the intruders.
- Image reconstruction quality obtained after decrypting the image.
- Storage size required to handle the bulk amount of data

Hence, it is understood that an optimal algorithm which performs an encryption and compression sequentially is the primary motive. Instead of a combined algorithm, even a sequential step by step process of encryption and compression is also sufficient, provided the overall security level for multimedia data access as the cloud environment has been increased. Compression and decompression methods are of two types namely, Lossy and Lossless. Lossy compressions are less significant in case of satellite and medical images. Lossy compressions are actually related to various frequency transformations which discards the high frequency information for the sake of better compression ratio. Hence, a proposal of using classification methods to classify the less significant and more significant features in the image, which would reduce the losses that occur in existing compression methods [1].

Intruders are discouraged through the improved metrics such as NPCR (Number of Pixels changing rate), UACI (Unified Averaged changed intensity) and mutual information among the lattices-based key. In the same way, image reconstruction quality is improved and verified through the metrics such as PSNR (Peak signal to noise ratio) and FOM (Figure of Merit). Compression performance is evaluated through the metric CR (Compression ratio). The performance is evaluated for both gray and color images medical data base under wireless channel environment [2].

IV. CONCLUSION

All the earlier works address the main problems such as key space, compression ratio. Only few literatures focused towards the mutual information between lattices, bifurcation diagram, KS entropy density, KS entropy generality, Space-Amplitude diagram and Space-Time diagrams. Total number of lattices in chaos state is an important problem in chaotic based encryption system. If not all the lattices are in chaos, it ends up in weak encryption system. The strength of encryption is determined only by these parameters mentioned above. Hence much importance is rendered to the calculation of such parameters will increase the performance of the system.Valleys existing in the KS entropy density and periodic windows in bifurcation diagram in the existing works clearly reveal that the existing secured systems are weak. Hence the major applications such as image recognition systems use authentication systems. Commonly available authentication systems utilize the biometrics r problem addressed in this research work is to reduce the number of valleys and shifting the valley to the higher magnitudes in KSE entropy density. Simultaneously eliminating the periodic windows in the bifurcation windows would automatically increase the strength of encryption. Besides this, mutual information among lattices are very useful to attackers to steal the original content. Hence lowering the mutual information among the lattices would make the intruders die due to the complexity in hacking. Along with this classification methods to classify the less significant and more significant features in the image, reduce the losses that occur in existing compression methods.

REFERENCES

[1] P. Manisekaran, M. R. A. Dhivakar and P. Kumar, "**Enhanced ImageEncryption using multiple iterated Arnold Coupled Logistic Map Lattices**," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 514-521, doi: 10.1109/ICCMC48092.2020.ICCMC-00096.

[2] P. Manisekaran, M. R. A. Dhivakar and P. Kumar, "**On the Analysis of Space-Amplitude Diagram in Chaotic based Image Encryption,**" 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 295-301, doi: 10.1109/ICESC48915.2020.9155605.

[3] P Manisekaran, P Dhankhar, and P Kumar, "**A Novel Approach to Improve Image storage and security by using Chaotic Image Encryption Method and lossless compression Method,**" ICTACT Journal on Image and Video Processing 11 (Issue - 2, November 2020, 2316-2324)

[4] Jalel Hajji, Mohamed Amine Ben Farah and Mounir Samet, AbdennaceurKachouri, "**Crypto-Compression of Images based on Chaos**," Proceedings of 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012, pp. 344- 350.

[5] Atef Masmoudi, William Puech, "**Lossless chaos-based crypto-compression scheme for image protection**," IET Image Process., 2014, Vol. 8, Iss. 12, pp. 671-686, doi:10.1049/iet-ipr.2013.0598.

[6] Guo, J.-I., & Yen, J.-C. (1999). "**A new mirror-like image encryption algorithm and its VLSI architecture**," Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China in 1999.

[7] Yen, J.-C., & Guo, J.-I. (2000). "**New chaotic key-based design for image encryption and decryption**," IEEE International Symposium on ISCAS 2000, Geneva (pp. IV-49- IV-52), May 2000.

[8] Sobhy, M. I., & Shehata, A. R. (2001). "**Chaotic algorithms for data encryption**," IEEE Proceeding of ICASSP 2001, Vol. 2, pp. 997-1000, May 2001.

[9] Masuda, N., &Aihara, K. (2002). "**Cryptosystems with discretized chaotic maps**," IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications, 49 (1), pp. 28–40.

[10] Sinha, A., & Singh, K. (2003). "**A technique for image encryption using digital signature**," Optics Communications, pp. 1–6. Retrieved from www.elsevier.com/locate/optcom.

[11] Zhang, Y., Xiao, D., Wen, W., & Tian, Y. (2013). "**Edge based light weight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform**," Optics & Laser Technology, 54, pp. 1-6.

[12] Ramahrishnan, S., Elakkiya, B., Geetha, R., Vasuki, P., Mahalingam, S. (2014). "**Image encryption using chaotic maps in hybrid domain**," International Journal of Communication and Computer Technologies, 2(5), pp. 44-48.

[13] Rhouma, R., Arroyo, D., &Belghith, S. (2009). "**A new color image cryptosystem based on a piecewise linear chaotic map**," In 6th International Multi-Conference on Systems, Signals and Devices, March 2009, pp. 1-6.

[14] Wong, A., & Bishop, W. (2007). "**Backwards compatible, multi-level region-of-interest (ROI) image encryption architecture with biometric authentication**," International Conference on Signal Processing and Multimedia Applications, July 2007, pp. 324-329.

[15] "**Image encryption by chaos mixing**," ISSN 1751-9659 Revised 16th March 2016 Accepted on 8th May 2016 doi: 10.1049/iet-ipr.2015.0244 www.ietdl.org Image Encryption using Chaos Theory, Yannick Abanda, Alain Tiedeu

[16] Robert, A., & Matthews, J. (1989). "**On the derivation of a "chaotic" encryption algorithm**," Cryptologia, XIII(1), pp. 29-42.

[17] Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1990). "**A secret key cryptosystem using a chaotic map**," Transactions of the IEICE, E73(7), pp. 1041-1044.

[18] Schwartz, C. (1991). "**A new graphical method for encryption of computer data**," Cryptologia, 15(1), pp. 43-46.

[19] Kuo, C. J. (1993). "**Novel image encryption technique and its application in progressive transmission**," Journal of Electronic Imaging, 2(4), pp. 345–351.

[20] Alexopoulos, C., Bourbakis, N., &Ioannou, N. (1995). "**Image encryption method using a class of fractals**," Journal of Electronic Imaging, 43, pp. 251-259.

[21] Yang, H.-G., & Kim, E.-S. (1996). "**Practical image encryption scheme by real-valued data**," Optical Engineering, 35(9), pp. 2473-2478.

[22] Baptista, M. S. (1998). "**Cryptography with chaos**," Physics Letters A, 240, pp. 50-54.

[23] Sallen, M., Ibrahim, S., &Isnin, I. F. (2003). "**Enhanced chaotic image encryption algorithm based on Baker's map**," IEEE Proceedings of ISCAS 2003, 2, pp. II-508–II-511.

[24] Shin, C.-M., Seo, D.-H., Chol, K.-B., Lee, H.-W., & Kim, S. J. (2003). "**Multilevel image encryption by binary phase XOR operations**," IEEE Proceedings in the year 2003.

[25] Belkhouche, F., &Qidwai, U. (2003). "**Binary image encoding using 1D chaotic maps**," IEEE Proceedings in the year 2003.

[26] Ying, W., DeLing, Z., Lei, J., et al. (2004). "**The spatial domain encryption of digital images based on high dimension chaotic system**," Proceedings of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, December 2004, pp. 1172–1176.

[27] Zhang, M.-R., Shao, G.-C., & Yi, K.-C. (2004). "**T-matrix and its applications in image processing**," IEEE Electronics Letters, 40(25), pp. 1583-1584.

[28] Deng, S., Zhang, L., & Xiao, D. (2005). "**Image encryption scheme based on chaotic neural system**," In J. Wang, X. Liao, & Z. Yi (Eds.) Advances in neural networks, ISNN 2005, LNCS 3497, pp. 868-872.

[29] Gu, G., & Han, G. (2006). "**An enhanced chaos based image encryption algorithm**," IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

[30] Xiao, H.-P., & Zhang, G.-J. (2006). "**An image encryption scheme based on chaotic systems**," IEEE Proceedings of the Fifth International Conference Machine Learning and Cybernetics, Dalian, pp. 13-16, August 2006.

[31] Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C., Wu, S. Y., Huang, C. K., et al. (2009). "**Hybrid image encryption using multi-chaos-system**," In 7th International Conference on Information, Communications and Signal Processing (ICICS), December 2009, pp. 1-5.

[32] Ahmad, M., &Alam, M. (2009). "**A new algorithm of encryption and decryption of images using chaotic mapping**," International Journal on Computer Science and Engineering, 2(1), pp. 46-50.

[33] Wei, W., Fen-lin, L., Xinl, G., &Yebin, Y. (2010). "**Color image encryption algorithm based on hyper chaos**," In 2nd IEEE International Conference on Information Management and Engineering, 2010,pp. 271–274.

[34] Sinha A., Singh, K. (2013). "**Image encryption using fractional Fourier transform and 3D Jigsaw transform**," Retrieved from http://pdf-world.net/pdf-2013/Imageencryption-using-fractional-Fourier transform-and-3DJigsaw- transform-pdf.pdf.

[35] Zhou, N., Wang, Y., Gong, L., Chen, X., & Yang, Y. (2012). "**Novel color image encryption algorithm based on the reality preserving fractional Mellin transform**," Optics & Laser Technology, 44(7), pp. 2270-2281.

[36] Abuturab, M. R. (2012). "**Securing color information using Arnold transform in gyrator transform domain**," Optics and Lasers in Engineering, 50(5), pp. 772-779.

[37] He, Y., Cao, Y., & Lu, X. (2012). "**Color image encryption based on orthogonal composite grating and double random phase encoding technique**," Optik (International Journal for Light and Electron Optics), 123(17), pp. 1592-1596.

[38] Chen, H., Du, X., Liu, Z., & Yang, C. (2013). "**Color image encryption based on the affine transform and gyrator transform**," Optics and Lasers in Engineering, 51 (6), pp. 768-775.

[39] Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., &Yunpeng, Z. (2010). "**A chaos-based image encryption algorithm using wavelet transform**," In 2nd International Conference on Advanced Computer Control, March 2010, Vol. 2, No. 4, pp. 217-222.