JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Survey on Chaos Based Image Encryption Techniques

[1]Falak Mittal, [2]Dr. Sanjay Dubey

[1]Student, [2]Assistant Professor
[1]Computer Science and Engineering,
[1]Amity University, Noida, India

Abstract : For a very long time, the security of picture data has been highly valued by researchers and information security specialists. The most straightforward and efficient method for ensuring the security of any given image information is image encryption. There are a number of more secure image encryption methods that have been suggested. Chaos based systems have been widely used in image encryption due to its intrinsic qualities including ergodicity, sensitivity to initial condition, and systematic parametrization. In this study, we examine various chaos-theory-based image encryption methods that offer high security.

***Index Terms* - Image encryption, chaos, substitution, neural network, permutation, cellular automata, DNA, entropy.**

I. Introduction

All There may be a high risk that an adversary may try to obtain sensitive information because of the growth of use of images for secure information transfer between two points via a network in sectors including telecommunications, online banking, defence, etc. The key goal is to use an algorithm to safeguard these photos so that a potential adversary cannot get any information from it. The topic of image encryption follows from this. Since chaos-based encryption is extremely sensitive to the starting circumstances, the periodicity. Compared to other encryption methods, it is more widely used. Chaotic maps are used often in encryption of images. Some examples include the tent, the logistic, and the sine maps.

A. *Logistic-Map*

It is a 2-degree polynomial mapping. Using the following equation, it may be illustrated:

$$x_n = r\, x_{n-1}(1 - x_{n-1})$$

where x ∈ [0, 1], n indicates how many iterations there have been, and values in the range [0, 4] of the parameter 'r' that are of interest.

B. *Tent-Map*

The equation below can be used to illustrate the tent map.:

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1 - x_n) & \text{for } \frac{1}{2} \le x_n \end{cases}$$

where r is a positive real number and xn is between 0 and 1.

C. *Sine-Map*

We produce a map that mimics logistic map, albeit with a distinct mathematical formula. It can be described using the equation below:

$$f_\mu(x) = \mu \sin(\pi x);\ \ x \in [0, 1],\ \ \mu > 0$$

The researchers covered in this paper often use the maps shown above. It is evident that [5-8] have encrypted images using a logistic map, [13-15] have used a tent map, and [9-12] have used a sine map.

To give the algorithm strong support and higher performance, many image encryption approaches combine chaos with one or more of the following methods.

The neural network (NN) is one of the methods. The field of image encryption uses NN since there is a high demand for its application in many different fields, and [21, 22] have proposed many techniques for encrypting images using NN.

An enhanced entropy-based image encryption method has been put forth by authors of [39, 40].

Permutation is yet another important method for image encryption. Thus, [23-28] implemented this to encrypt images. In order to reduce the relationship between neighbouring pixels, it is used.. Several authors [5, 8, 40, 34–36] have suggested using DNA sequences to encrypt images and have described their novel, distinctive approaches.

Numerous research projects have been carried out utilizing a range of approaches, such as hyper-chaos (for illustration, see [8, 38]); and the method widely used in [16-20] is substitution.. Furthermore, [29, 30] provide a thorough overview of chaos-based cryptography.

In this research, we examine chaos-based encryption methods, which are motivated by the dynamical behaviour of the chaotic systems that are susceptible to the beginning parameters. Any algorithm for image encryption should be resistant to an attack. Most often, the manner in which encryption methods are designed leads to diffusion and confusion. while encrypting data in order to meet this goal.

Thus, any encryption scheme may be made better by using both of these procedures. These two stages give every encryption method the strongest possible defence against common assaults. Additionally, in chaotic cryptography-based encryption of images, the pixels of the image are scrambled by creating random orders. So, in this paper, we discuss different chaos-based image encryption methods.

II. RESEARCH METHODOLOGY

Present evaluation technique is associated with the literature assessment that objectives diverse research questions to find out, compare, select out and incorporate all the excessive fantastic research proof critical for the research. Its aim is to present an honest assessment of research issue remember with the aid of way of the usage of a taken into consideration worthy, rigorous, and auditable method. Among the available methodologies, paper chooses the journals and studies paper methodologies. Lot of previous papers in the associated subjects are identified at unique stages. In the making plans of the evaluation, the want for the assessment is diagnosed, the studies questions are unique, and the evaluation protocol is defined. Now while enticing within the assessment, the preliminary research are determined on, the feature evaluation requires research are described, the statistics abstraction is finished, and the received facts are then analyzed. Finally, even as describing the evaluation phase, the publishing mechanisms are exceptional, and the evaluation document is ready. In this evaluation, we take into consideration the papers from 2016-2022 as more work is available in these years.

III. LITERATURE REVIEW

In this section, we categorise the chaotic cryptography based encryption algorithms using a variety of approaches that fall under the chaos domain, including shuffling, DNA, the logistic map, the chaotic map, the tent map, the sine map, etc.

2.1 Algorithms employing Chaotic Map for Image Encryption

The authors present a novel technique for creating an efficient and straightforward chaotic system by comparing output sequence of 2 identical one-dimensional chaos-based maps that are already in existence in paper [1]. Numerous tests and computer simulations have shown that suggested system produces 1D chaos-based system with better performance, and, wider ranges.. A new linear-nonlinear-linear that is based on total shuffling has been introduced to demonstrate its use in picture encryption. Numerous testing and analysis show that the system offers high security levels and is resistant to statistical assaults.

Ahmad and Hwang in their study [2] offer a chaotic picture encryption technique with a larger keyspace utilising affine transformations. Even one round of encryption can yield a larger keyspace. By utilising addition and XOR to generate random sequences, the connections between the pixels are broken. The cypher picture is obtained via affine transformations to ensure the algorithm's resistance against various attacks. The algorithm passes numerous tests and is found to be resistant to assaults such as differential and plain image, among many others. This approach was feasible and secure due to the characteristics of chaotic maps and its sensitivity to the initial conditions.

The authors have suggested ways to improve the chaos techniques now in use to produce chaotic sequences that aid with encryption in paper [3]. To overcome the drawbacks of existing techniques, they have here offered two distinct Integrated Chaotic Systems (ICS). The switch operations, the cascades were tried on one dimensional chaotic maps and resulted in a better and more intricate chaotic map. With the help of ICS, they created an image encryption method to demonstrate the effectiveness of the upgraded chaotic systems. The method is resistant to several assaults and has a sizable keyspace.

A specialized discrete chaos-based map namely "2D-TFCDM" that makes use of discrite fractional calculus has been introduced by authors in their publication [4]. A numerical examination of the chaotic behaviour is also performed. The bifurcation diagram and phase portrait are then shown. The final step is to convert discrite fractional map into the algorithmic steps by utilizing an elliptic curve to create keys in a finite field.

2.2 Algorithms employing Logistic Map for Image Encryption

Authors have added to a paper that was previously published on encryption of images using one dimensional chaos map and DNA algorithms in paper [5]. The plain images are encrypted with DNA using a chaos-based map before the mask is created. Following the DNA addition principles, the resultant mask is then mixed with the previously created DNA encoded picture. DNA complementation, an intermediary step in the process of picture encryption, uses a complementary matrix together with 1D chaotic maps. The suggested approach may be reversed entirely and is resistant to common attacks like plaintext and statistical ones.

The authors propose a novel spatiotemporal chaos-based method that uses a dynamically coupled logistic-map lattices in paper [6]. A chaotic area has a bigger parameter space and is deemed more chaotic than the typical Lattice, according to many tests and analyses. A dynamic coupled technique has been created to achieve this. As a result, this paper introduces and illustrates bit-level encryption of images.

Authors presented a 2D Sine Map that has been adjusted logistically in paper [7]. Studies have shown that compared to many of the chaos-based maps that have already been made, it is more unpredictable and has a larger range. Using the provided map, this research also creates 2-dimensional LASM employing picture encryption method. The source of diffusions, and, confusions is categorically eliminated, and a technique for enhancing the security of the cypher picture involves adding random data points to plain pictures. Experimental findings show that the suggested approach may successfully protecting the pictures by encrypting those into cypher pictures.

In their study [8], the authors utilized multi-dimensional chaos-based systems and cyclical processes to encrypt DNA pictures. The pixels of the picture are randomly encoded using DNA coding rule, and Chen's hyper-chaotic keystream records this operation. The Lorens systems are used for reducing connections between neighbouring pixels so as to provide safe encryption. The diffusion process is carried out via XOR method for binary matrixes, and decoding resulting in the cypher picture. Simulations are used to show the resistance of the encryption algorithm against exhaustive, differential, statistical, and assaults with a higher level of security.

2.3 Algorithms employing Sine Map for Image Encryption

A brand new two-dimensional Chebyshav Sine map which has been naturally graded has been presented by the authors in paper [9]. Based on the map, a color picture encryption cypher was developed. Before every encryption operation, coloured non Gaussean noise is used to produce the beginning condition. XOR process and avalanche effect can be combined to get desired outcome after two iterations. Many research and simulations show that this method may be utilised for encrypting pictures delivered via cloud since it is quick.

Authors have used the idea of perturbation, which is the deviation of things from their courses in paper [10]. Additionally, methods for choosing dynamic state variables are used during the picture encryption process. A 2D modified sine map is used to produce random numbers. It proposes auxiliary variables utilised for orbital deviations of chaos-based map. Previous pixels are to blame for this variance. To create the keystream, a state variable is also picked. The developed approach is secure since the image can accept both plain and cypher pictures.

A novel technique employing two dimensional Sine-Iterative chaos-based Map with Innumerable Collapsible Modulations has been proposed and its randomness has been evaluated using a number of analytical tests in paper [11]. To increase the key space, one can first create a two dimension Sine Modulations map. For creating disorder in image, chaos based shift transformation methods have been employed for changing the picture's positions of pixels while also exchanging rows with columns. Diffusions and confusions processes happen simultaneously in this situation. Finally, the image is encrypted using a combination decomposition technique.

Authors propose a novel 1D logistical map using 1D chaotic map's output sequences in paper [12]. Through comparison study, it was demonstrated that the new chaotic map was more accurate. This research also proposes a chaotic picture encryption strategy employing enhanced chaotic map. Numerous studies and experiments have demonstrated that this encryption technique offers effective defence against a variety of assaults.

2.4 Algorithms employing Tent Map for Image Encryption

A Chaos-based Tent Map (CTM) has been employed to construct a modified picture encryption procedure in paper [13]. A novel and improved approach that randomly generates streams of key streams for image encryption is obtained by reconstructing the CTM. A 1D CTM is used to generate the keystream, which takes less time to execute and offers higher security. To provide secure encryption, this algorithm's intermediary phases alter the original conditions and parameters.

To encrypt the colour image, a chaotic tent map was made by employing objective bits plane technique in paper [14]. The received original picture is divided in eight planes of eight bit, and those planes have then been categorised as significant or non-significant using an experimentally inferred threshold figure of 0.3. Second, using sequences of keystreams, all significant bits are encrypted. Since only the significant planes of bits are encrypted, one can see that the computational complexity is minimised in this situation.

Authors have provided a method for compressing and encrypting colour photographs in paper [15]. Fuzzy splines are employed to compress images firstly. Then, a new chaotic combination system has been presented for encrypting pictures using chaotic systems. Additionally, 3D shift in the encryption process maybe present. The effectiveness, security of the provided method have been demonstrated by analyses and simulations.

2.5 Algorithms employing Substitution for Image Encryption

The authors propose a novel picture encryption approach using chaos-based systems, substitution, and combination network in paper [16]. There are four distinct cryptography steps. Diffusion is the initial step, which has been built using a brand-new chaos-based map. Then, a diffusion step using chaos-based logistical map has been presented. This will significantly improve the encryption's performance. Last but not the least, a combination step is accomplished using a combination function to improve the performance of the approach. Various tests, studies, and experiments were carried out to show that the suggested encryption approach offers strong security.

The authors have demonstrated the encryption of colour images cypher with a replacement keystream generation technique in paper [17]. Chaos-based Lu model is used for creating create a substitution and permutation keystream sequence by combining and scrambling picture data. The two main issues with discretised form of areas preserving chaos based maps have been avoided with the utilisation of a pixel-exchange method to shuffle the locations of coloured subpixels in the input image. In the substitution stage of the iterative logistic map, an efficient keystream construction technique has once again been proposed that can generate three keystream elements. Experimental findings have demonstrated that this method offers an adequate level of security and outperformed more traditional techniques in efficiency.

The authors have suggested a fast and safe image encryption technique in paper [18]. This approach uses one dimensional chaos based system that had been created using an old one dimensional chaos based map that had flaws in its characteristics although superior qualities within the bounds of the parameters. The newly imagined chaotic system will be generating a random number sequence, and the S-box has already been created. Then a novel technique of plain picture substitution was utilised to boost overall security. After that, a scrambling method is used utilising the S-box that was previously constructed. Different testing and evaluation metrics have demonstrated the proposed technique to be dependable and secure.

Authors presented a novel binary tree traversal approach for comprehensive encryption and decryption in paper [19]. In actuality, it employs four block cyphers, each of which uses bit level substitutions and permutation components to encrypt a block of data at a time. To fix the issues with file size, this binary tree approach is utilised. In parameters like time taken for execution, processing power used, speed of execution, the suggested technique outperforms numerous well-known algorithms.

Images have been encrypted using logistic chaotic maps and dynamic substitution boxes (DSB) in paper [20]. A permutation is divided into blocks throughout the diffusion process, and each block is diffused individually using DSB, improving the overall security. At the end, all of the blocks combine to create the cypher image. Experimental evidence demonstrates the algorithm's resilience to attacks and its ability to transmit data over an insecure channel.

2.6 Algorithms employing Neural Network for Image Encryption

Authors propose a chaotic encryption technique that uses neural networks for encrypting images in paper [21]. A composite chaos based map combined with the tent maps and logistic maps is employed to obtain the initial key. The photos are then jumbled during the transformational step using the Armold map. The chaotic matrix is produced using Hopfield neural network techniques; once more, the transformation function provides the key. Now that the final key has been obtained, the obtained chaotic matrix is XORed with it to produce a cypher image. This algorithm turned out to be resistive after many analyses on noise, cutting, and many other things.

A novel technique for the encryption of images is presented by authors in the paper [22]. In their approach, the authors create a random list of prime numbers using a seed, and successive lists are created recursively. As a result, recursive seeding is employed for generating numbers randomly rather than a single direct seed. Every pixel of a picture’s then encrypted with an equivalent pixel in initial picture for reducing the likelihood of starting picture may be derived without keys being acknowledged. This scheme's robustness has been demonstrated through a variety of studies and tests.

2.7 Algorithms employing Permutation for Image Encryption

Typically, papers discuss encryption procedures including confusion and diffusion as distinct steps. Here, authors develop a crypto-system in which diffusion and confusion occur at the same time in paper [23]. They have employed the Permutasion Diffusion Operation, which allows simultaneous diffusion and confusion, improving the encryption process's accuracy. When compared to the current approaches, this algorithm is more efficient in terms of execution time, is resilient against picture noise, and performs better in many other areas.

Typically, we discover image encryption approaches where all 3 colour component experience diffusion and confusion process. However, authors have given us a technique in which we can combine those into 3 bit-level permutasions to generate a bit-level picture in paper [24]. Next, we use permutation methods and chaos-based systems to encrypt the bit-level image that has just been created. Experimental evidence shows that because the components are handled independently, this technique takes less time to execute. As a result, when the image is encrypted, the quality is improved.

Authors have suggested improving an encryption technique that employs cyclical rotations, confusion, and diffusion for encrypting images in paper [25]. They illustrate assaults that earlier algorithms were vulnerable to and offers better approach. The presented technique deals with two directional diffution and various permutasion strategies that are resistant to assaults such keyspace based on plain picture, as seen in algorithm which were proposed earlier. Experimental evidence shows the proposed technique offers higher security than previously proposed algorithms.

Contrary to existing studies, the authors here offer a non chaos-based image encryption technique that uses permutation in paper [26]. One can see how cyclic group attributes can be used to create a permutation (sequence). This continues through the stages of bewilderment and diffusion (which produce unpredictability). Although the algorithm's susceptibility to threats is unclear, it has been found to be faster and more secure than many other existing algorithms.

The authors use Henon Chaos-Based Map algorithm and secret keys 128 bits in size in paper [27]. The Henon map, which generates random numbers using this process, only exhibits chaotic behaviour for a specific set of constants, and it is also very sensitive to the initial parameters, which means that it changes dramatically even when the parameter values are only slightly altered. In order to give a broader key space, a 128-bit secret key is employed in addition to the Henon map. After then, pixels are mixed up using the HCM's permutation matrix.

Authors have presented a straightforward chaotic-based picture encryption technique that seeks to offer great security and effectiveness in paper [28]. The metrics of cat map employed in this cryptosystem are linked to the plain images. Both the permutation and diffusion stages in this cryptosystem involve plain images. This relationship results in increased sensitivity, which makes this cryptosystem effectively resistant to differential or chosen/known plaintext attacks. The algorithm has undergone extensive testing and is resistant to numerous attacks.

2.8 Algorithms employing Cellular Automata for Image Encryption

Authors have offered a variety of safe techniques to transmit images in paper [29]. Authors develop a equitably distributed two dimensional chaotic map for increasing the security. Cellular automata and discrete framelet transform are also used, and position of each pixel is then intermixed by using different types of shifts. The proposed technique is demonstrated to give good security against a number of assaults.

Li et al. [30] is a supplementary to the work on encryption using hybrid hyper chaos-based systems that was previously proposed. Previously, putting aside the secret keys, the product of values at every index of the pixel is calculated for the beginning condition for encryption. Value of every component of pixels can now be changed with the equivalent permutation keystream given, as long as the product of the values of the pixel at every colour remains fixed. Additionally, the theoretical and experimental analyses of the algorithms were conducted.

The authors offer a novel neural network-based picture encryption method in paper [31]. It uses a sampled-data controller and is created by synchronising various time delays. The chaos based systems play a significant part in securing the communication. Because of higher accuracy of FCNNs, using them for processing of images is preferable. Then, using FCNNs, chaotic values are collected and used to encrypt images. The image is encrypted by performing the aforementioned processes. This method has been proven to be effective against a variety of attacks through various simulations and tests.

The authors have presented a hybrid cellular automata (HCA) and depth-conversion integral imaging (DCII) technique-based safe picture encryption method in paper [32]. Using DCII techniques, the original image is broken up into an Elementary Image Array (EIA) in this procedure. Next, cellular automata and chaos are used to encrypt the EIA. As it moves into the resolution reduction phase, image quality is reduced using computational imaging techniques and then improved during decryption using a depth conversion system. The algorithm has a wide keyspace and is sensitive to keyspaces.

Authors have presented a revolutionary Cellular Automata (CA)-based picture encryption method in paper [33]. The suggested plan makes use of dispersal and confusion. The chaos mapping replaces the indices of the pixels throughout confusion phase. The key picture is formed by employing nonuniform CA and the the hyperchaotic mapping are utilised for choosing random integers for encrypting from the picture’s key. Due to its large keyspace, nearly optimal entropy, and great encryption efficiency, this approach provides security.

2.9 Algorithms employing DNA for Image Encryption

The authors present an algorithm that encrypts colour images using DNA computations and Chen’s systems in paper [34]. Chaotic sequences have been created using the Chen technique. The mean value of each pixel in a colour image serves as the beginning point for the Chen system, ensuring that various original images have various secret keys. The provided approach is suitable for colour image encryption, according to experiments. As a result, the given technique improves security and thwarts various assaults.

Authors have devised an image encryption method that boosts the unpredictability and confidentiality of the image using DNA encoding and Rivest Cipher (RC4) in paper [35]. Even while this plan boosts security, it has no impact on quality. The effectiveness of the plan is estimated using a variety of tests. This method has been proven to be effective against a variety of attacks and highly secure through various simulations and tests.

The authors have presented a picture encryption algorithm that makes use of DNA coding methods and Lorenz Hyper-Chaotic Systems (LHCS), which produce high unpredictability and low correlation coefficient in paper [36]. The SHA-256 technique is employed to generate a secret key, and LHCS can be used to discover the initial values required to build the DNA sequence matrix and the dynamic S-box. Then, to provide unpredictability into the images, DNA sequences are used in conjunction with S-box and SCAN. It can be seen from the simulation that this algorithm is reliable and efficient.

Authors have suggested a novel encryption method that is built using a combination of cellular automatas, DNAs, and the Tinkerbells chaos-based map in paper [37]. The CA regulations, the DNA regulations, DNA sequences, and the XOR operators are simultaneously utilised for encrypting the pixels of plain pictures. Numerous experiments and analyses have demonstrated that this approach is resistant to many assaults and has great encryption.

Wang and Zhang have proposed a genetic recombination and hyperchaos-based image encryption technique in paper [38]. To construct chaos (unpredictability) images, they used the fundamental genetic recombination processes. The diffusion and permutation process follows, which offers extra security. The hyper-chaotic Lorenz systems produce pseudo-random numbers.

2.10 Image Encryption Algorithms based on Entropy

Authors propose a chaos-based map and information entropy-based image encryption technique in paper [39]. Operations including modulation, permutation, and diffusion are used in this approach. By doing so, the suggested approach avoids the flaw of the traditional methods, which required that the pixel locations be strictly shuffled before diffusion. The usage of information entropy is then employed to influence keystream generation. The cypher functions as an indiscrete unit that increases security since the starting keys used during the permutation and diffusion steps interact with one another. Results of many tests and analysis show that the given encryption does a decent job of successfully safeguarding the images.

Images are encrypted by simultaneously using a chaotic system, information entropy, and, DNA encoding in paper [40]. Because of the sensitivity and unpredictability to changes, the chaotic system offer higher security. By dividing each pixel into four pieces and performing diffusion and confusion operations, DNA encoding is carried out. IE is employed to strengthen the algorithm's resistance to plain-text attacks and to increase its sensitivity to modifications. When it comes to decryption, the performance would be impacted. The algorithm has been proven to be resistant to various attacks through various simulations and tests.

2.11 Miscellaneous

Authors have presented a novel picture encryption technique that concentrates on the transmission of pictures to earth via satellites in paper [41]. This system's primary responsibility is to ensure that data confidentiality is upheld during the entire procedure. Earlier, systems based on chaos were utilised to maintain privacy in this way. This study presents a novel Fridrich's scheme-based multispectral image encryption technique. The proposed strategy has been proven to be highly secure through various studies.

A double encryption technique has been proposed by the authors in paper [42]. This approach uses the Blowfish cypher and Cross Chaos Map because they are resistant to cryptanalysis assaults. The parameters for the method's effective operation are the Unified Average Changed Intensities, the Amount of Pixels with Changed Rate, and the Coefficient of Correlation. It is demonstrated through various tests and analyses that this method offers good security.

Authors have put forth an improved encryption algorithm that combines a parallel encryption process based on chaos and a Randomised Number Generator for quick, effective picture encryption in paper [43]. RNG is utilised in this instance to spread confusion, which leads to encryption of the picture’s pixels. They also employ parallel encryption, because it considers each of the thread individually, to further improve the algorithm's security and speed of execution. It is demonstrated through various tests and analyses that this method minimises the execution time. This approach is very helpful when there are very huge data sets that have to be encrypted.

The authors have presented a brand-new hybrid encryption technique based on chaos that is intended to successfully and securely encode images in paper [44]. Due of its dynamic properties, Zhongteng chaotic system is chosen for outlining the method. The S-Boax algorithm is developed, and its performance is examined. The novel hybrid picture encryption technique, built on AES, is created utilising the S-Box and RNG algorithms. It is demonstrated through various tests and analyses that this method is more secure and, efficient according to the results.

Double Random Phase Encoding (DRPE) using various blocks of different sizes is explored and proposed by authors as an opto-color cypher in paper [45]. By first splitting the colour image into identically sized blocks and then employing an optical emitter, the colour image is transformed into an optical signal. Phase modulation and Fourier domains are two different forms of time that are used in the DRPE approach. The optical encryption image is then converted to digital representation using a charge-coupled device camera. This suggested DRPE-based strategy has been demonstrated to be efficient and secure through many testing and analyses.

Contrary to others, the authors provide a clever technique for double encryption in which the Reversible Watermarking (RW) algorithm and chaos is employed for verifying the authenticity of decrypted picture in paper [46] .They first incorporate the data into the original image using the RW method, and then they diffuse the image using chaotic techniques. To generate the Verifiable Encrypted Image, RW was once more utilised to embed information from the diffused image (VEI). A complete decryption would result from changing or tampering with the VEI, providing sufficient data security. In the fields of medical science, the defence, and the satellite communication, this method has a wide range of applications.

Bit-level encryption was developed by Xu L and Gou X which uses Cyclic Shifts, swapping, and Peicewise Linear Chaos-Based Map (PWLCM) in paper [47]. 2 binary sequence are created from plain picture using bit-plane decomposition. After that, a diffusion approach is used to make the sequences responsive to image changes. One round of execution of the proposed technique is found to make the encryption more secure. The algorithm has undergone extensive testing and is resistant to numerous attacks.

The following Table 1 represents the summary of findings from literature review.

References	Authors	Technique	Findings
[2]	Ahmad J, Hwang SO	Chaotic map	Higher keyspace and the algorithm is resistant to frequently used attacks.
[8]	Hou S, Li Z, Gong JH, Oyang BS	Logistic map	It is proven to achieve unpredictability, wider chaotic range, and a good ergodicity.
[10]	Lu J, Wang Z, Li Z	Sine map	To prevent potential attacks, multiple iterations of diffusion and confusion are carried out at bit-level. But, The method has a high correlation coefficient.
[13]	Lu D, Zhang G, Qin L	Tent map	Offers enhanced security and speedy execution.
[20]	Rahman Ali, Hassan SJ, Ahmed K,	Substitution	Increases security order in unsafe lines. The method, however, is highly susceptible to error.
[21]	Wang XY, Li ZM	Neural network	Offers higher obscurity, great security, high speed. However, the method is challenging and prone to errors.
[24]	Teng L, Wang X, Meng J	Permutation	Simple and safe against many frequent attacks. The technique, though, is slow and underwhelming.
[29]	Khedmati Y, Parvaz R, Behroo Y	Cellular automata	Provides a keyspace structure that is dynamic. However, the algorithm is very lengthy.
[34]	Liu L, Zhang Y, Zhang H	DNA	Offers high entropy and a very low correlation coefficient. But. it is not a method that is cost-effective.
[40]	Zhou J, Wang G, Min Lu, Jinming I	Entropy	Algorithm is made more change-sensitive, and robustness against plain-text attack is offered.
[44]	Çavao¸su ˘glo Ü, Kaçer S, Jengin D, Pahlivan K	S-AES	Better memory use compared to the AES method, good time performance. However, memory utilisation can be cut even more.
[38]	Wang X, Zhang HL	Hyper-chaos system	Large keyspace, quick processing, and strong security. However, the process is convoluted and takes too long.
[47]	Zu Li, Jou, Li Zhou, Li Jintao	Block-based transformation	Large keyspace as well as high efficiency,strong security, and integration with cloud settings. However, the likelihood of a key generation error is significant.

TABLE I. SUMMARY OF LITERATURE REVIEW

IV. CONCLUSION

We have examined a variety of recent chaos theory-based schemes of encryption of images in this paper. Due to the chaos theory's strengths in the areas of ergodicity, control parameters, pseudo-randomness, and periodicity. It also has a high sensitivity to initial conditions. Table 1 shows the techniques of encryption of images covered in this paper produce good results. In terms of speed, time complexity, etc., there is still room for implementation in a few algorithms. For instance, it is clear from the studies [1, 33], that these encryption techniques still require refinement. A totally secure strategy may be difficult to propose due to the proliferation of image decoding methods. As a result of the foregoing, we can draw the conclusion that when formulating a chaos-based picture encryption scheme, one should consider cryptanalysis in order to prevent leakage.

REFERENCES

[1] Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. Sig Process 138:129–137
[2] Ahmad J, Hwang SO (2016) A secure image encryption scheme based on chaotic maps and affine transformation. Multimed Tools Appl 75(21):13951–13976

[3] Lan R, He J, Wang S, Gu T, Luo X (2018) Integrated chaotic systems for image encryption. Sig Process 147:133–145
[4] Liu Z, Xia T (2018) Novel two dimensional fractional-order discrete chaotic map and its application to image encryption. Appl Comput Inf 14(2):177–185
[5] Jain A, Rajpal N (2016) A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools Appl 5455–5472
[6] Xingyuan W, Le F, Shibing W, Zhang C, Yingqian Z (2018) Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access 6:39705–39724
[7] Hua Z, Zhou Y (2016) Image encryption using 2D logistic-adjusted-sine map. Inf Sci 339:237–253
[8] Hu T, Liu Y, Gong LH, Ouyang CJ (2017) An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dyn 87(1):51–66
[9] Liu H,Wen F, Kadir A (2019) Construction of a new 2D Chebyshev-Sine map and its application to color image encryption. Multimed Tools Appl 78(12):15997–16010
[10] Li H, Wang Y, Zuo Z (2019) Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. Opt Lasers Eng 115:197–207
[11] Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36
[12] Pak C, An K, Jang P, Kim J, Kim S (2019) A novel bit-level color image encryption using improved 1D chaotic map. Multimed Tools Appl 78(9):12027–12042
[13] Li C, Luo G, Qin K, Li C (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dyn 87(1):127–133
[14] Som S, Mitra A, Palit S, Chaudhuri BB (2019) A selective bitplane image encryption scheme using chaotic maps. Multimed Tools Appl 78(8):10373–10400
[15] Zarebnia M, Kianfar R, Parvaz R (2019) Multi-color image compression-encryption algorithm based on chaotic system and fuzzy transform. Multimed Tools Appl 78(8):10491–10511
[16] Belazi A, El-Latif AA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Sig Process 128:155–170
[17] Fu C, Zhang GY, Zhu M, Chen Z, Lei WM (2018) A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy. Secur Commun Netw
[18] Nkandeu YPK, Tiedeu A (2019) An image encryption algorithm based on substitution technique and chaos mixing. Multimed Tools Appl 78(8):10013–10034
[19] Priya A, Sinha K, Darshani MP, Sahana SK (2019) A novel multimedia encryption and decryption technique using binary tree traversal. Springer, Singapore, pp 163–178
[20] Rehman AU, Khan JS, Ahmad J, Hwang SO (2016) A new image encryption scheme based on dynamic s-boxes and chaotic maps. 3D Res 7(1):7
[21] Wang XY, Li ZM (2019) A color image encryption algorithm based on Hopfield chaotic neural network. Opt Lasers Eng 115:107–118
[22] Annadurai S, Manoj R, Jathanna RD (2018) A novel self-transforming image encryption algorithm using intrinsically mutating PRNG. In: Proceedings of first international conference on smart system innovations and computing, pp 203–214
[23] Huang L, Cai S, Xiong X, Xiao M (2019) On symmetric color image encryption system with permutation-diffusion simultaneous operation. Opt Lasers Eng 115:7–20
[24] Teng L, Wang X, Meng J (2018) A chaotic color image encryption using integrated bit-level permutation. Multimed Tools Appl 77(6):6883–6896
[25] Chen J, Han F, Qian W, Yao YD, Zhu ZL (2018) Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map. Nonlinear Dyn 93(4):2399–2413
[26] Kandar S, Chaudhuri D, Bhattacharjee A, Dhara BC (2019) Image encryption using sequence generated by cyclic group. J Inf Secur Appl 44:117–129
[27] Mishra K, Saharan R (2019) A fast image encryption technique using henon chaotic map. In: Progress in advanced computing and intelligent engineering. Springer, Singapore, pp 329–339
[28] Huang L, Cai S, Xiao M, Xiong X (2018) A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion. Entropy 20(7):535
[29] Khedmati Y, Parvaz R, Behroo Y (2018) 2D hybrid chaos map for image security transform based on framelet and cellular automata. arXiv preprint arXiv, 1810.06333
[30] Li M, Lu D, Wen W, Ren H, Zhang Y (2018) Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. IEEE Access 6:47102–47111
[31] Kalpana M, Ratnavelu K, Balasubramaniam P, Kamali MZM (2018) Synchronization of chaotic-type delayed neural networks and its application. Nonlinear Dyn 93(2):543–555
[32] Li X, Li C, Lee IK (2016) Chaotic image encryption using pseudo-random masks and pixel mapping. Sig Process 125:48–63
[33] Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyperchaotic system and cellular automata. Opt Lasers Eng 90:225–237
[34] Liu L, Zhang Y, Zhang H (2018) A color image encryption algorithm based on DNA computation and Chen system. J Phys Conf Ser 1074(1):012096
[35] Hameed SM, Sa'adoon HA, Al-Ani M (2018) Image encryption using DNA encoding and RC4 algorithm. Iraqi J Sci 59(1B):434–446
[36] Cui G, Wang L, Zhang X, Zhou Z (2018) An image encryption algorithm based on dynamic DNA coding and hyper-chaotic lorenz system. Springer, Singapore, pp 226–238
[37] Enayatifar R, Sadaei HJ, Abdullah AH, Lee M, Isnin IF (2015) A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt Lasers Eng 71:33–41
[38] Wang X, Zhang HL (2016) A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. Nonlinear Dyn 83(1–2):333–346
[39] Ye G, Pan C, Huang X, Zhao Z, He J (2018) A chaotic image encryption algorithm based on information entropy. Int J Bifurc Chaos 28(01):1850010

[40] Zhen P, Zhao G, Min L, Jin X (2016) Chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl 75(11):6303–6319

[41] Bensikaddour EH, Bentoutou Y, Taleb N (2018) Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher. J King Saud Univ Comput Inf Sci

[42] Bora S, Sen P, Pradhan C (2016) Novel color image encryption technique using Blowfish and Cross Chaos map. In: 2015 international conference on communications and signal processing (ICCSP), pp 0879–0883

[43] Çavu¸so ˘glu Ü, Kaçar S (2019) A novel parallel image encryption algorithm based on chaos. Cluster Comput 1–13

[44] Çavu¸so ˘glu Ü, Kaçar S, Zengin A, Pehlivan I (2018) A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dyn 92(4):1745–1759

[45] Faragallah OS, Alzain MA, El-Sayed HS, Al-Amri JF, El-Shafai W, Afifi A, Soh B (2019) Block-based optical color image encryption based on double random phase encoding. IEEE Access 7:4184–4194

[46] Gao H, Gao T (2019) Double verifiable image encryption based on chaos and reversible watermarking algorithm. Multimed Tools Appl 78(6):7267–7288

[47] Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52