A Novel Image Encryption Technique using Multi-Coupled Map Lattice System with Generalized Symmetric Map and Adaptive Control Parameter

SN Computer Science (2023) 4:81
https://doi.org/10.1007/s42979-022-01503-4

ORIGINAL RESEARCH

A Novel Image Encryption Technique Using Multi-Coupled Map Lattice System with Generalized Symmetric Map and Adaptive Control Parameter

Syed Muhammad Unsub Zia[1] · Mark McCartney[1] · Bryan Scotney[1] · Jorge Martinez[1] · Ali Sajjad[2]

Received: 16 December 2021 / Accepted: 10 November 2022

Abstract
Image and video data make up a significant portion of the content shared over the Internet and social media. The use of image and video communication allows more information to be shared while simultaneously presenting higher risks in terms of data security. The traditional encryption schemes are general purpose; however, to encrypt image and video data, application-specific encryption solutions are needed. An image or a video frame comprises a two-dimensional matrix where pixel intensity values are integers in range [0,255], leading to data redundancy problems. Moreover, the bulk amount of image and video data adds another challenge when deploying security primitives. In this paper, a novel coupled map lattice system-based image cryptosystem has been proposed that uses generalised symmetric maps for generation of pseudo-random sequences. The generalization of symmetric maps allows the user to choose the source of pseudo-random sequence generation by varying a single control parameter. Other adaptive control parameters ensure an adequate degree of randomness in the generated sequences. The proposed encryption system relies on three independent sources of pseudo-random sequence generators, which are further re-randomized before the final encryption process. Comprehensive experimentation has been performed to test the proposed system against various attack models on publicly available datasets. A detailed comparative analysis has also been conducted with existing state-of-the-art image encryption techniques. Results show that the proposed algorithm provides high information entropy, negative correlation, large key space, and high sensitivity to key variations, and is resistant to various types of attacks, including chosen-text, statistical, and differential attacks.

Keywords Coupled map lattice · Generalised symmetric map · Cryptography · Image encryption

Introduction

Chaos was brought to prominence by Lorenz more than a half century ago, and has been studied extensively since then [1]. Over this time, the concepts of chaos theory have been applied to an increasing number of concrete systems, including, as is discussed in this paper, cryptography [2]. The research in chaotic systems ranges from low-dimensional to high-dimensional systems with complex chaotic behaviour [3]. In a recent study, we surveyed existing state-of-the-art chaos-based encryption schemes for image data that have been applied in spatial, temporal, and spatiotemporal domains [4]. Further research led to the exploration of spatiotemporal systems commonly known as Coupled Map Lattices (CMLs), that exhibit highly complex behaviour in discrete time, discrete space, with continuous state. In early literature, CML systems have been successfully applied in the fields of pattern dynamics [5–12] and vacuum fluctuations in high-energy physics [13]. The Japanese scientist Kaneko created the diffusive CML model, which is one of the most studied CMLs [14]. Despite the fact that the proposed model by Kaneko generates quite complex spatiotemporal chaos, in terms of cryptography, it has shortcomings [15]. In particular, the CML system may have a limited range of parameter space which is chaotic which can limit its applications in the field of cryptography due to a restricted key space.

Researchers have come up with numerous solutions to improve the spatiotemporal behaviour of CML systems and also improve the region of parameter space for which

✉ Syed Muhammad Unsub Zia
zia-smu@ulster.ac.uk

[1] Ulster University, Belfast, Northern Ireland, UK

[2] Applied Research, British Telecom, Ipswich, UK

Published online: 06 December 2022

the CML is chaotic. In 2011, a Globally Non-local Coupled Map Lattice (GNCML) model was proposed [16]. The authors in [17, 18] introduced a One-Way Coupled Map Lattice (OCML) and Two-Way Coupled Map Lattice (TCML), respectively. The idea of a stochastic-based coupled map logistic map lattice was presented by Sinha et al. [19]. Some researchers improved Sinha's model, and some introduced new stochastic coupled logistic models [20–23]. The above-mentioned CML versions are based on non-adjacent lattices that are randomly generated and are not restorable, and thus, despite the improvements, their use is greatly restricted. Later, Zhang et al. proposed a mixed linear-nonlinear coupled map lattice [24] and an Arnold Coupled Logistic Map Lattice (ACCML) [25]. Some published work exists on different dimensional systems, Kaneko et al. introduced one and two-dimensional lattice systems [26], Muruganandam et al. presented low-dimensional behaviour in a three-dimensional CML system [27], whereas Zhang et al. proposed a CML system in four-dimensional space [28]. Furthermore, the above-mentioned publications are based on static coupling CML systems. Xingyuan et al. proposed a CML system based on dynamic coupling coefficients which can be abbreviated as Logistic Dynamic Coupled Map Lattice (LDCML) [29].

Despite the improvements suggested by researchers for CML systems, there is still a need to address the issue of the range parameter space for which CML lattices exhibit chaos. The majority of the proposals discussed above use the logistic map as the local map for the CML system. The logistic map is a second-order map that belongs to the family of symmetric maps [30]. In an earlier study, we proposed the idea of generalised symmetric maps to be used as local maps instead of the logistic map. Another contribution of that study was to introduce the idea of adaptive control parameters that would increase the probability that the CML system remains in the chaotic zone for a larger range of parameter choices. This study was implemented to generate pseudo-random sequences for Internet of Things (IoT) sensor devices. In the present work, we have extended the proposed idea to image encryption as an application of information security. Since there has already been significant work done in the field of image encryption, we contribute here by proposing a new image encryption algorithm that comprises multiple CML systems. The proposed encryption algorithm has been validated on different datasets and tested for different type of attacks. The results prove that the proposed encryption algorithm is quite robust to various types of attacks and holds a large key space which makes it a stronger candidate compared to existing algorithms with smaller key space.

The rest of this paper is organized as follows: in the section "Related work", related works are discussed. In the section "A CML model with GSM and adaptive control parameter", the CML model with Generalised Symmetric Map (GSM) and adaptive control parameters is explained. In the section "Analysis of proposed system", the behaviour of the proposed CML system is analysed and explained. The section "Application in image in encryption" comprises the new image encryption algorithm and its testing against various types of benchmarks. Finally, in the section "Conclusion", the conclusion of the study is put forward.

Related Work

In 2016, Hao et al. proposed a one-dimensional CML system as an application to image encryption [31]. Whereas, in 2020, Sun et al. introduced a two-dimensional non-adjacent coupled map lattice model [32]. The proposed CML system was used for image encryption, where a chaos-based mixed scrambling technique was used for pixel shuffling and knight's tour method was used for image diffusion. The initial values for scrambling and diffusion were seeded from the proposed CML system.

In 2014, Ying et al. presented a symmetric image encryption scheme based on mixed linear-nonlinear coupled map lattices [33]. They introduced another coupling parameter and two additional control parameters to the original CML system proposed by Kaneko. The values of the control parameters were generated using the Arnold cat map. They applied the proposed idea to generate a 400-bit long key to encrypt and decrypt images. In 2016, the authors tried to improve the previously proposed system and added DNA sequence encoding rules to randomize the generated key from the CML framework [34].

The complexity of DNA sequences makes them a suitable candidate to be used with CML systems for image encryption. Li et al. proposed a secure and efficient algorithm for image encryption based on DNA encoding and coupled map lattices [35]. In another study, the authors used DNA coding with bitwise XOR operations to encode the image and used a CML system for row and column shuffling [36]. Zhen et al. further introduced an image encryption scheme that combined spatiotemporal chaos, DNA sequences, and entropy [37]. In 2017, a research article on an image cryptosystem was published that used DNA insertion and deletion for the encryption process [38]. They also suggested modifications to the CML system by deploying the logistic-sine system (LSS) instead of the logistic map conventionally used. Recently, an image encryption and transmission strategy was proposed using DNA encryption and a double chaotic system [39]. The term double chaos means that it comprises of two different chaotic sources, namely: (1) an optical chaotic system and (2) a coupled map lattice system. The proposed model comprises master and slave lasers to generate optical chaos, a coupled map lattice chaotic system,

and DNA complementary rules to generate a 128-bit encryption/decryption key.

CML and DNA sequences were collectively used recently in a study for colored images [40]. The three color components from a colored image are extracted to form a matrix, on which a confusion operation is applied using CML sequences and permutation is applied using DNA sequences. In another study on color images, DNA encryption was proposed using a CML system and one-time keys [41]. The proposed idea relies on generating keys using an SHA-256 hashing function, converting the color components into DNA matrices. Confusion and permutation are then performed on the combined DNA matrix, applying DNA addition, subtraction, and XOR operations to DNA blocks, and final transformation of DNA matrices to decimal matrices. The authors in [42] introduced a customized globally coupled map lattice for color image encryption. A key image of the same size as the original image is created and the values for the key image are populated using a logistic map. The key image is shuffled and replicated into four images of the same size. A confusion phase is performed, and one of the four images is chosen as the key image, whereas the other three images are combined to create a cipher image.

There have been several other interesting advancements in image encryption schemes involving CML systems. A recent study proposed a hybrid model of a modified genetic algorithm and coupled map lattices to encrypt medical images [43]. The authors in [44] proposed a fast image encryption technique that utilizes non-adjacent dynamically coupled map lattices. Wang et al. used nonlinear diffusion-based multiple coupled map lattices to perform image encryption [45]. In another study, the authors tried to rectify the problem of key diffusion for encrypted images [46]. They suggested the replacement of half transient iterations with the iterations form coupled map lattices. In a study for color image encryption, the authors introduced a cryptosystem based on coupled map lattices and a fractional-order chaotic system [47]. They also proposed a different shuffling method for the permutation–diffusion phase, in which the original image is segregated into four subparts, and then, the positioning in the whole image is shuffled. Some researchers also used statistical concepts for image encryption. In [48], a new image encryption method has been introduced combining coupled map lattices and the Markov properties. They claimed that the kind of chaos generated using Markov properties has higher complexity than logistic or tent maps.

Considering the literature discussed in this section, it can be deduced that in most of the proposals, the image encryption algorithms have been intentionally made complicated and computationally hefty. In some cases, the image is copied four times and further operations applied on them are overheads. Using already existing techniques like DNA sequences, Arnold cat maps, and Markov models in conjunction with a CML system is arguably, not necessary, as a CML system alone is capable of generating complex and pseudo-random sequences that could form a robust cryptosystem. Also, in the context of CML system improvement, some researchers presented solutions with CML systems using non-adjacent lattices, dynamic coupling, and so on, but they do not necessarily contribute towards increasing the key space of the cryptosystem. In this study, we propose a very simple and novel image encryption algorithm which uses multiple CML systems to generate a strong cipher image. The CML system used for image encryption is also novel, as its local maps are based on generalised symmetric maps (GSMs) proposed in a recent study [49]. The CML system relies on an adaptive control parameter which increases the probability that the CML system stays in chaotic region for a larger fraction of parameter choices.

A CML Model with GSM and Adaptive Control Parameter

In the spatiotemporal system proposed in this paper, the local maps are chosen from the family of symmetric chaotic maps. We generalise the choice of symmetric chaotic maps by allowing the user to simply choose the value of α to select a map from symmetric chaotic maps family. This increases the map options to choose from, whereas in conventional CML systems, usually logistic map is used. This liberty of options to choose local maps in turn increases the key space for the CML system. We also propose the idea to make the control parameter corresponding to chosen α value to be adaptive, which automatically tunes itself to keep the selected chaotic map above the accumulation point. This improves the overall behaviour of the CML system and increases the likelihood of the generation of highly chaotic and complex sequences.

CML Systems

There exists a series of studies on spatiotemporal systems from the 1980s that were applied to electrical circuitry, but, as noted earlier, Kaneko is credited with the introduction of the CML model as it is commonly defined [50]. The CML model can be visualised using the difference equation (1) that presents the diffusive CML model [51]

$$x_{n+1}(i) = (1-\epsilon)f(x_n(i)) + \frac{\epsilon}{2}[f(x_n(i+1)) + f(x_n(i-1))]. \tag{1}$$

Equation (1) shows a two-way diffusive CML model, where every node of the lattice is linked to left and right neighbouring nodes with a coupling factor (ϵ). Parameter i denotes the present node, where $(i-1)$ and $(i+1)$ refer to the left and right neighbouring nodes, respectively. The value of i ranges between $(1 \leq i \leq N)$ where N is the number of lattice

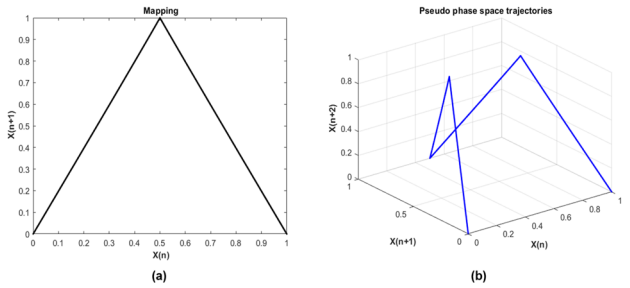

Fig. 1 **a** Mapping and **b** pseudo-phase space trajectory of the first-order tent map

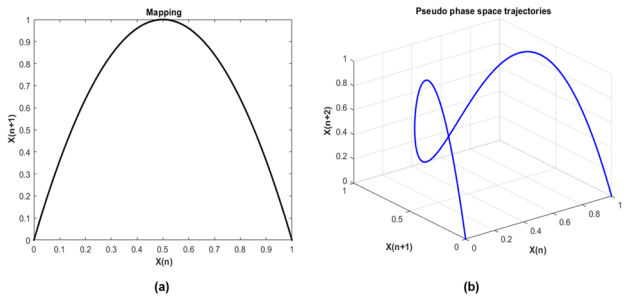

Fig. 2 **a** Mapping and **b** pseudo-phase space trajectory second-order logistic map

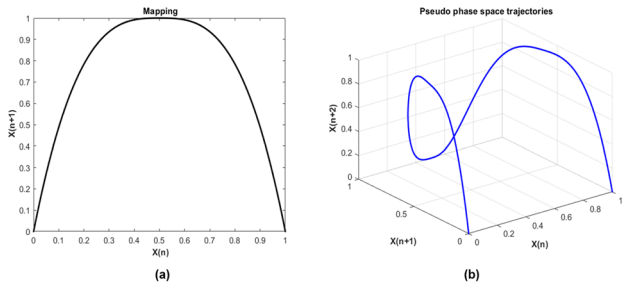

Fig. 3 **a** Mapping and **b** pseudo-phase space trajectory of the third-order symmetric map

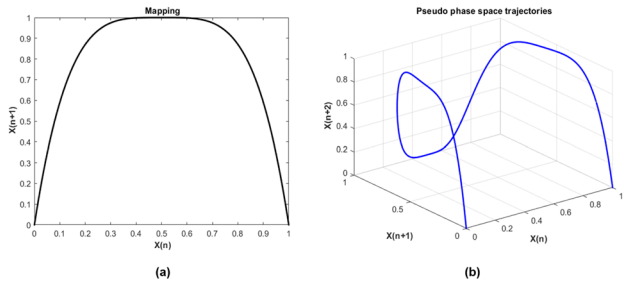

Fig. 4 **a** Mapping and **b** pseudo-phase space trajectory fourth-order quartic map

points in the CML . ϵ is the coupling factor that links lattices together and ranges between [0,1]. The system has discrete time steps with the current time denoted by n. The $f(x)$ is the local map function for the CML system, which is traditionally the logistic or tent map, but in the proposed model, $f(x)$ is chosen as a GSM. The lattice points in the CML system follow looped structure, which means that the first and last nodes of the lattice are linked together. For instance, in a CML system with ten lattice points ($N = 10$), and the present lattice number i is also 10. Then, the neighbouring nodes for 10th lattice point would be $(i - 1)$, i.e., $10 - 1 = 9$th lattice point and $(i + 1)$, i.e., $10 + 1 = 1$st lattice point.

Generalised Symmetric Maps (GSM)

The generalised symmetric map is defined over the unit interval as

$$f(x) = \beta(1 - |1 - 2x|^{\alpha}), \tag{2}$$

where α represents the order of the map which we restrict to the range [0.5,4], while β is the control parameter that ranges between [0,1]. Figures 1, 2, 3 and 4 show the mappings and pseudo-phase space trajectories for symmetric maps. Figure 1 represents first-order tent map which can be simply used by setting the value of α to 1 in Eq. (2). Figure 2 shows second-order logistic map, Fig. 3 shows third-order symmetric map, and Fig. 4 shows the fourth-order quartic map.

Any of these maps, or other maps from symmetric maps family can simply be used by setting the α value to a map order number in Eq. (2). Thus, the parameter α produces a selection of symmetric maps to choose from, which contribute towards a larger key space for the CML-based cryptosystem.

Adaptive β

In general , chaotic maps only exhibit chaotic behaviour over a range initial conditions and control parameters. The point at which the chaotic map first moves into chaotic zone from a non-chaotic region is termed the accumulation point (a) for that map (Fig. 5).

For the logistic map, α is set to 2 and the accumulation point lies between 0.89 and 0.90 (0.8925 to four decimal places). Furthermore, to calculate the accumulation trend for other symmetric maps, we analyse their Lyapunov exponents [52]. The Lyapunov exponent allows us to quantify the chaotic behaviour of a map, as positive Lyapunov values represent chaos and negative values show non-chaotic behaviour.

The variation of accumulation point with control parameter α is shown in Table 1. For the purpose of the image encryption algorithm, we consider α to be $(0.5 \leq \alpha \leq 4.0)$ to have positive and consistent α values that produce chaotic

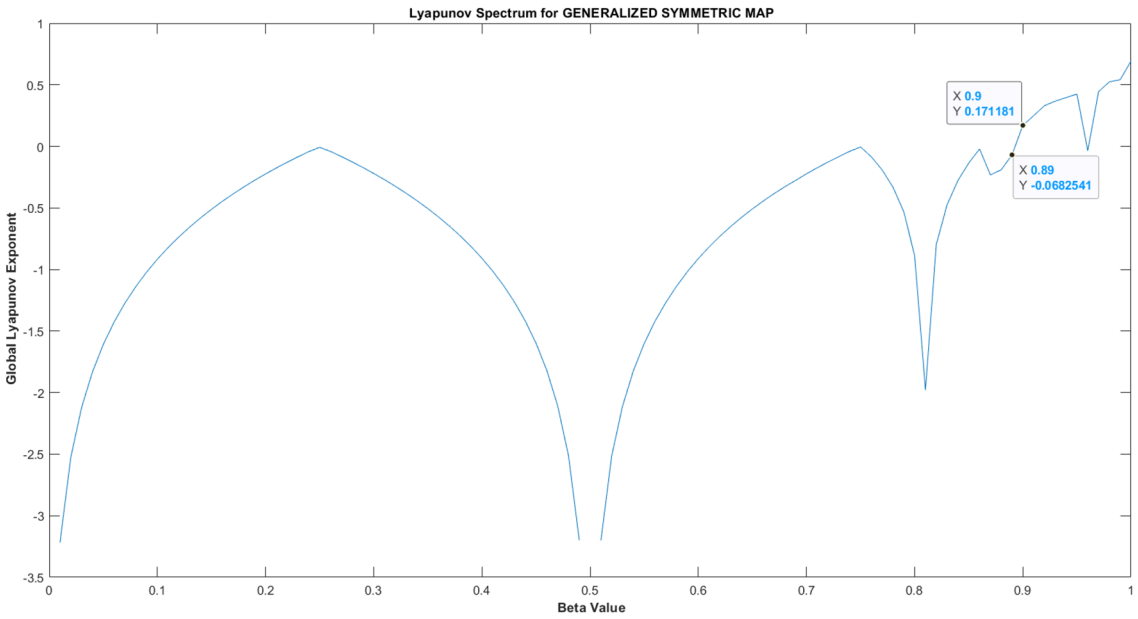

Fig. 5 Accumulation point for logistic map and represents the relationship between Lyapunov exponents and Accumulation points (a)

Table 1 Accumulation point value for corresponding α values

Control parameter (α)	Accumulation point (a)
0.25	Non-chaotic
0.5	1.0
0.7	0.72
1.0	0.50
1.5	0.82
2.0	0.90
2.5	0.93
3.0	0.95
3.5	0.97
4.0	1.0

behaviour. To further visualise the trend of accumulation points with respect to α values, we perform interpolation of points, as shown in Fig. 6. It can be seen that for any value of α, there is a corresponding accumulation point value.

To further ensure that the map chosen in Eq. (2) remains in chaos for majority of time, we introduce a concept of an adaptive β. The adaptive β can be represented using Eq. (3)

$$ad_{\beta i} = a + (1 - a)(1 - \epsilon^{-\gamma i}), \tag{3}$$

where a is the accumulation point value, and γ is a new tuning parameter introduced to control the spread of values and should be positive ($\gamma > 0$). i denotes the present lattice value and ($ad_{\beta i}$) is the adaptive β ranging between $a \leq ad_{\beta i} \leq 1$. Equation (3) does not guarantee chaos, but ensures that the control parameter remains above the accumulation point value and below 1, which increases the possibility of a system to be in the chaotic zone.

Analysis of Proposed System

A thorough analysis was performed to analyse the behaviour of the CML system with the GSM as local map and adaptive β values being used. One of the most reliable measures is to observe the Kolmogorov–Sinai (KS) entropy behaviour of the system [53]. The entropy patterns of the system can identify the chaotic and non-chaotic zones based on the control parameters and initial conditions. Another tool to study the characteristics of a system is to analyse the bifurcation diagrams [54]. Bifurcation diagrams can be plotted for every individual lattice to inspect its behaviour. In the next subsection, detailed results on KS entropy and bifurcation analysis have been provided.

Kolmogorov–Sinai Entropy Analysis

In one of the early studies published by Kaneko, he explained the information flow and Lyapunov analysis specifically for coupled map lattices [55]. For an N-dimensional CML system, there exist N Lyapunov exponents for the system. To obtain the Lyapunov spectra of the CML system, the product of Jacobi matrices J_p is required which could be calculated using Eq. (4)

$$J_p = \lim_{n \to \infty} J_n . J_{n-1} . J_{n-2} ... J_2 . J_1, \tag{4}$$

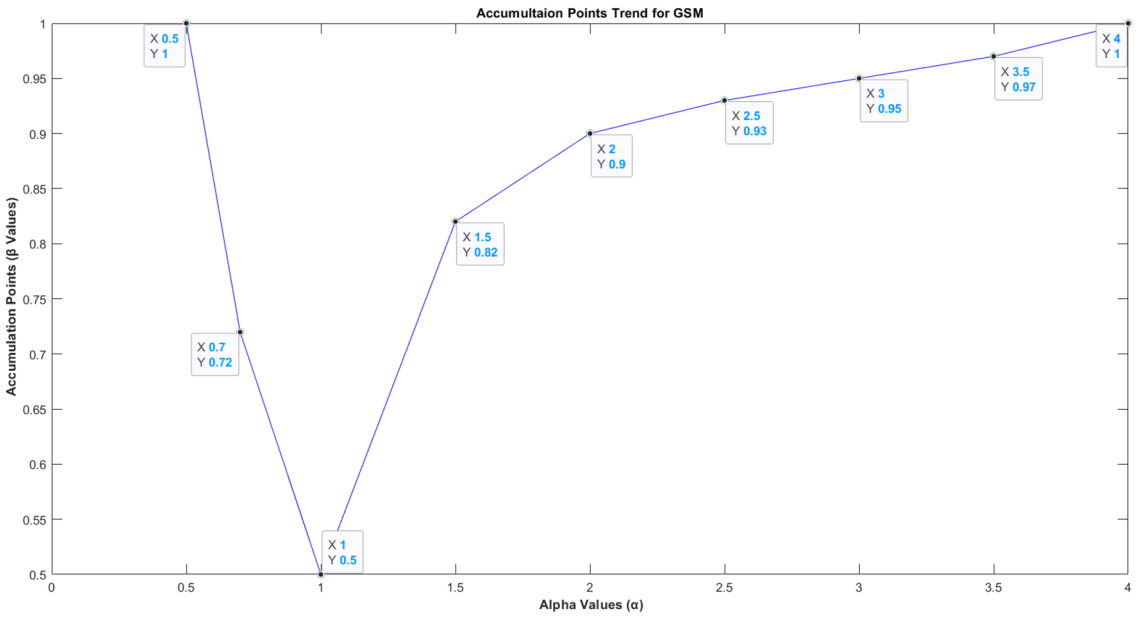

Fig. 6 Accumulation point trend for corresponding α values

where n is referred to the time step and J_n is the single Jacobian calculated at time step n. The product of all individual Jacobians leads to Jacobi product (J_p). Once eigenvalues are extracted from J_p, calculating natural logarithm of the eigenvalues results in Lyapunov exponents as shown in Eq. (5)

$$\lambda_i = \left(\frac{1}{n}\right) \ln(|\text{eigenvalues}(J_{pi})|). \tag{5}$$

In above equation, λ_i refers to the ith Lyapunov exponent ordered as $\{\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N\}$, this set defines the Lyapunov spectra. To calculate the KS entropy for the system, the sum of positive Lyapunov exponents is divided by the dimension of the system

$$h_\mu = \frac{1}{N} \sum_{\lambda_i > 0} \lambda_i. \tag{6}$$

In the above equation, N denotes the dimension of the CML system, λ_i refers to the positive Lyapunov exponents, and h_μ is the KS entropy density for the system. To analyse the KS entropy density of the CML system, we perform several experiments with varying parameters.

Figures 7 and 8 shows some results from the KS entropy density analysis; Fig. 7 is the KS entropy plot for a system with 50 lattice points, 500 initial discarded iterations, 1000 calculated iterations and γ set to 0.15, whereas Fig. 8 shows the KS entropy diagram for a system with 150 lattice points, 500 initial discarded iterations, 1000 calculated iterations and γ set to 0.15. Few empty regions can be observed close to a coupling factor ($\epsilon \cong 0.15$) and corresponding values for α in range ($1.5 \leq \alpha \leq 4$), and these areas represent non-chaotic zones. Whereas, for the ϵ in range [0,0.1] and [0.2,1], the trend of entropy density is very stable, and the system is in chaos with high entropy values. The results from Figs. 7 and 8 also show that increasing the number of lattices smooths the entropy plots. It can be also deduced from KS entropy density experiments that overall the CML system with GSM and adaptive β is chaotic for the majority values with the exception of a small region at coupling factor ($\epsilon \cong 0.15$).

Bifurcation Analysis

The KS entropy density analysis discussed in the previous section presents an idea of the overall system entropy behaviour, whereas with bifurcation diagram, detailed system behaviour of individual lattices can be studied. The bifurcation diagram for each lattice point was plotted for increasing α values on the x-axis in range [1,4], across the values generated by the CML system on the y-axis ranging between [0,1]. Figure 9 shows the bifurcation diagrams visualised for a system with 50 lattice points, 1000 initial discarded iterations, 2000 calculated iterations, and γ value 0.15. Figure 9 has further been segregated on the basis of 1st, 25th, and 50th lattice plots shown as the columns of the figure, and the rows denote increasing coupling factor values ($\epsilon = 0.2, 0.5$ and 0.8). Similar experiments were performed for the CML system with 150 lattice points, 1000 initial discarded iterations, 2000 calculated iterations, and γ set to 0.015.

Following the same pattern to analyse the first, middle, and last lattice point, bifurcation diagrams in Fig. 10 show the behaviour of a CML with 150 lattice points.

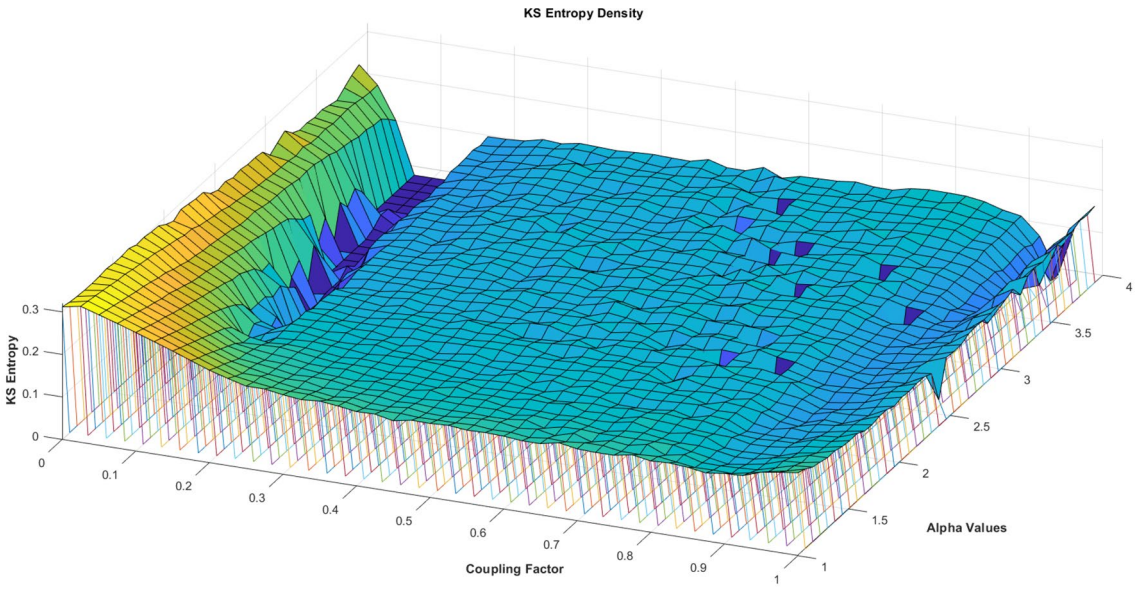

Fig. 7 KS entropy plots for CML systems with 150 lattices, for 500 initial discarded iterations, 1000 calculated iterations, $[0.5 \leq \alpha \leq 4]$, coupling factor $[0 \leq \epsilon \leq 1]$, and β adaptive

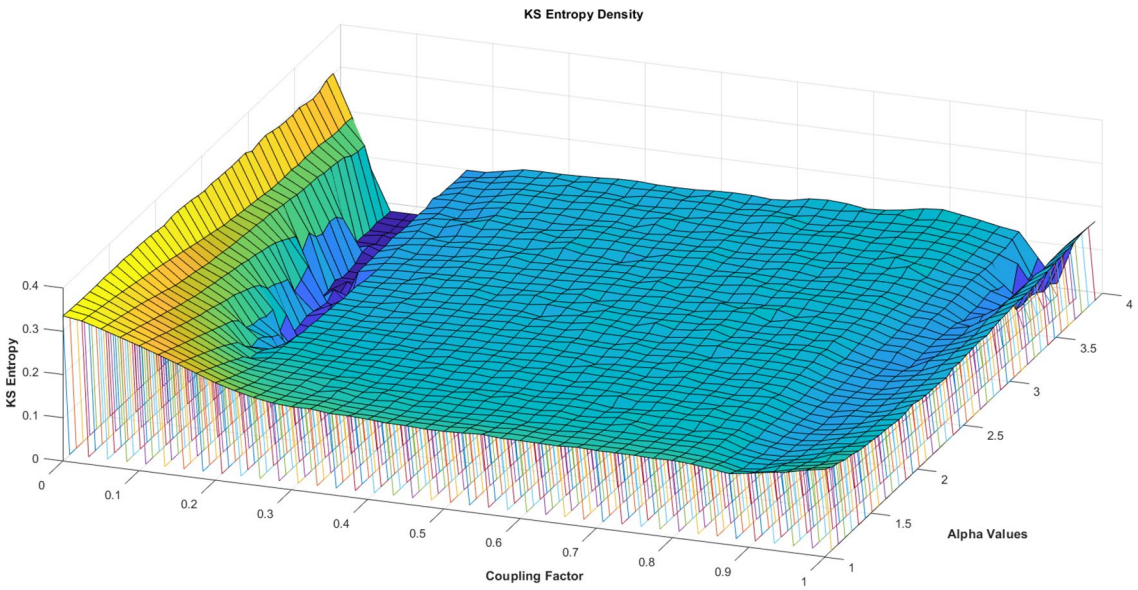

Fig. 8 KS entropy plots for CML systems with 50 lattices, for 500 initial discarded iterations, 1000 calculated iterations, $[0.5 \leq \alpha \leq 4]$, coupling factor $[0 \leq \epsilon \leq 1]$, and β adaptive

Application in Image in Encryption

The arrival of high-speed Internet has allowed digital media (specially images and videos) to be easily accessed by the general public. This great facility comes at the cost of great risk, as multimedia data contain a much higher amount of information than text. There are several traditional encryption schemes available, for instance; Advanced Encryption Standard (AES) and Data Encryption Standard (DES), but they might not be the best fit for image or video encryption purposes. Some inherent properties of images such as high redundancy in pixel data and bulk data capacity make them different from normal text data [56]. Unlike plain text, an image comprises of a two-dimensional matrix where pixel intensity values, that are integers in [0, 255], lead to data redundancy problems. The use of conventional encryption techniques can leave a

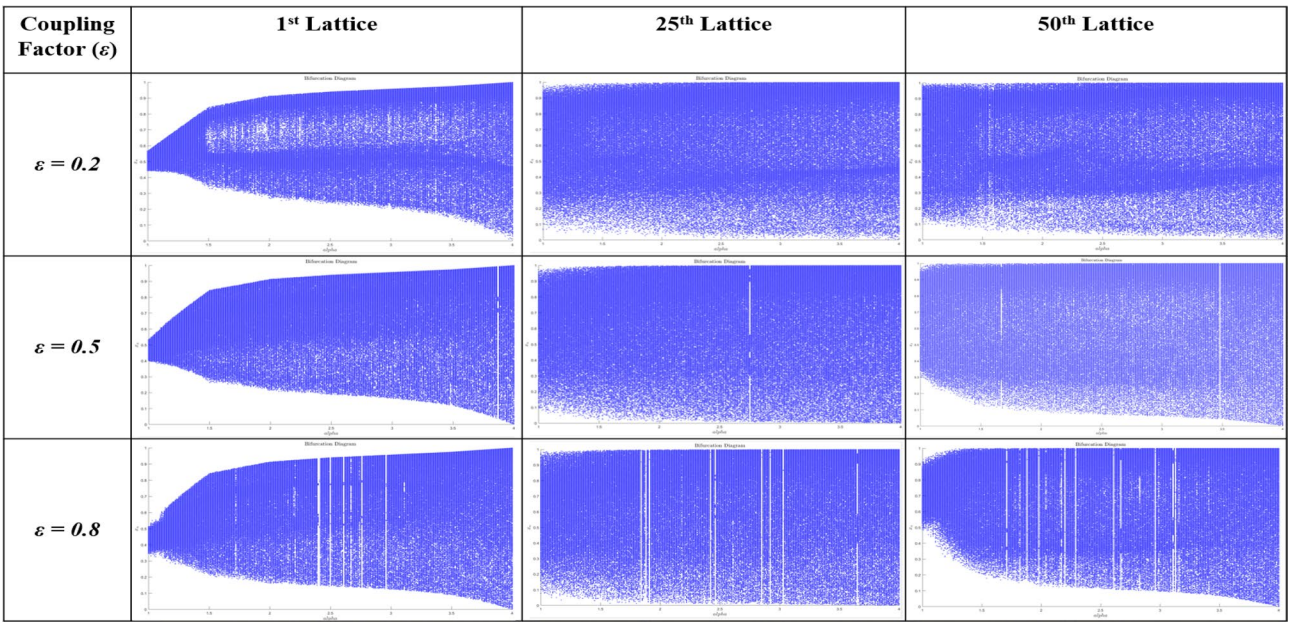

Fig. 9 Bifurcation diagrams for CML system with 50 lattice points for increasing coupling factor and different lattice numbers

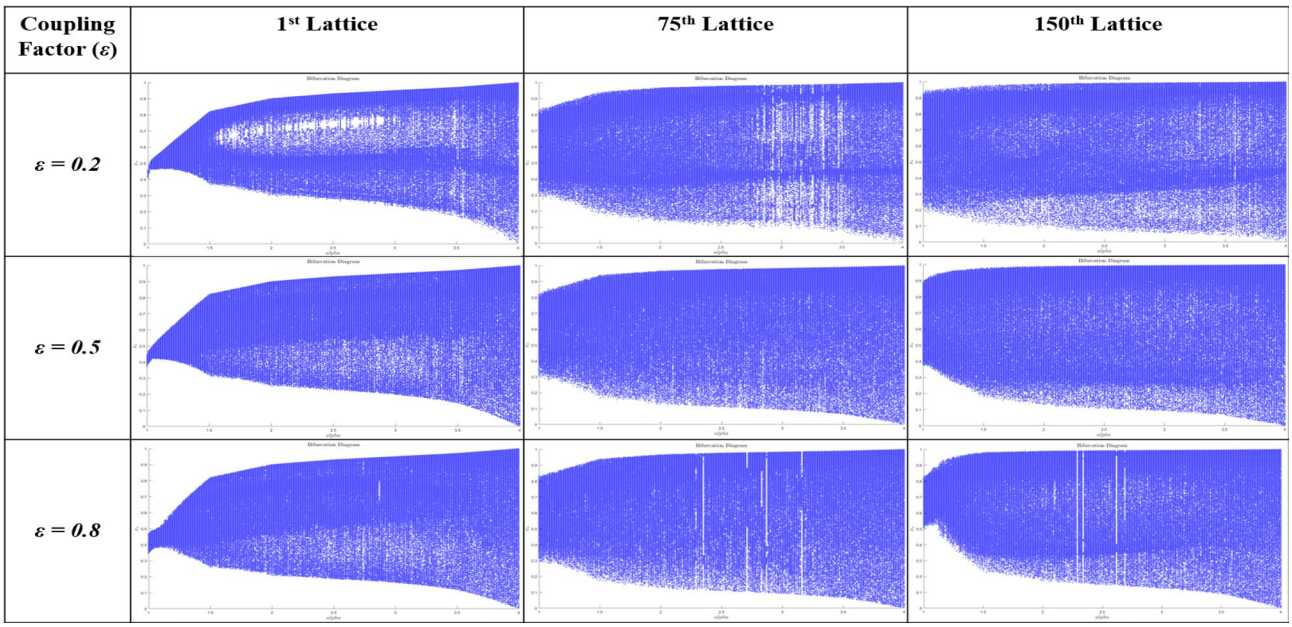

Fig. 10 Bifurcation diagrams for CML system with 150 lattice points for increasing coupling factor and different lattice numbers

pattern that could be exploited if a value is repeated several times in the ciphertext. These facts lead to the need of developing a cryptosystem able to encrypt every pixel value using a unique key and able to generate a random patterns in the ciphertext.

Algorithm Description

Figure 11 shows the overall hierarchy of the modules involved in the proposed image encryption system. This framework comprises three independent CML systems that

generate pseudo-random sequences based on different key parameters. These pseudo-random sequences are further re-randomized to ensure randomness of the generated pattern. Based on the pseudo-random sequences, confusion and permutation operations are performed. A separate module for XOR operations adds another layer of security. For all these operations, separate sequences from independent CML systems are used, which makes the system complex and hard to guess the seed key values. The encryption and decryption processes and their working is explained in the next section.

Encryption Process

The overall encryption process comprises of six main steps:

STEP 1: Image pre-processing

- The original image is converted from RGB to grayscale for processing.
- In this paper, a weighted method has been used which converts RGB values to grayscale values by forming a weighted sum of the Red (R), Green (G), and Blue (B) components as: 0.2989 * R + 0.5870 * G + 0.1140 * B.

STEP 2: Key initialization

- For the proposed system, initial conditions and control parameters for the CML system act as encryption keys.
- There are three independent CML systems in the proposed model, and therefore, they need separate inputs to generate unique pseudo-random sequences.
- The key inputs for all three CML system are as follows: CML1: $x1(0)$, $i1$, $\alpha 1$, $\beta 1$, $\gamma 1$, $\epsilon 1$, CML2: $x2(0)$, $i2$, $\alpha 2$, $\beta 2$, $\gamma 2$, $\epsilon 2$, and CML3: $x3(0)$, $i3$,$\alpha 3$, $\beta 3$, $\gamma 3$, $\epsilon 3$.

STEP 3: Pseudo-random sequences generation using multi-CML system

- CML system 1, 2, and 3 are supplied with the initialization parameters as shown in step 2.
- CML system 1, 2, and 3 output unique pseudo-random sequences X1, X2, and X3, respectively.

STEP 4: Re-randomization of CML system output sequences

- For re-randomization of the CML sequences, another control parameter (R) is introduced which also contributes towards the encryption key.
- CML sequences $X1$, $X2$, $X3$ and $R1$, $R2$, $R3$ are given as input to the re-randomization module $Y = (\text{round}(X * Rmod(256))$.
- The above equation generates $Y1$, $Y2$ and $Y3$ as final pseudo-random sequences to be used for encryption.

STEP 5: Confusion phase

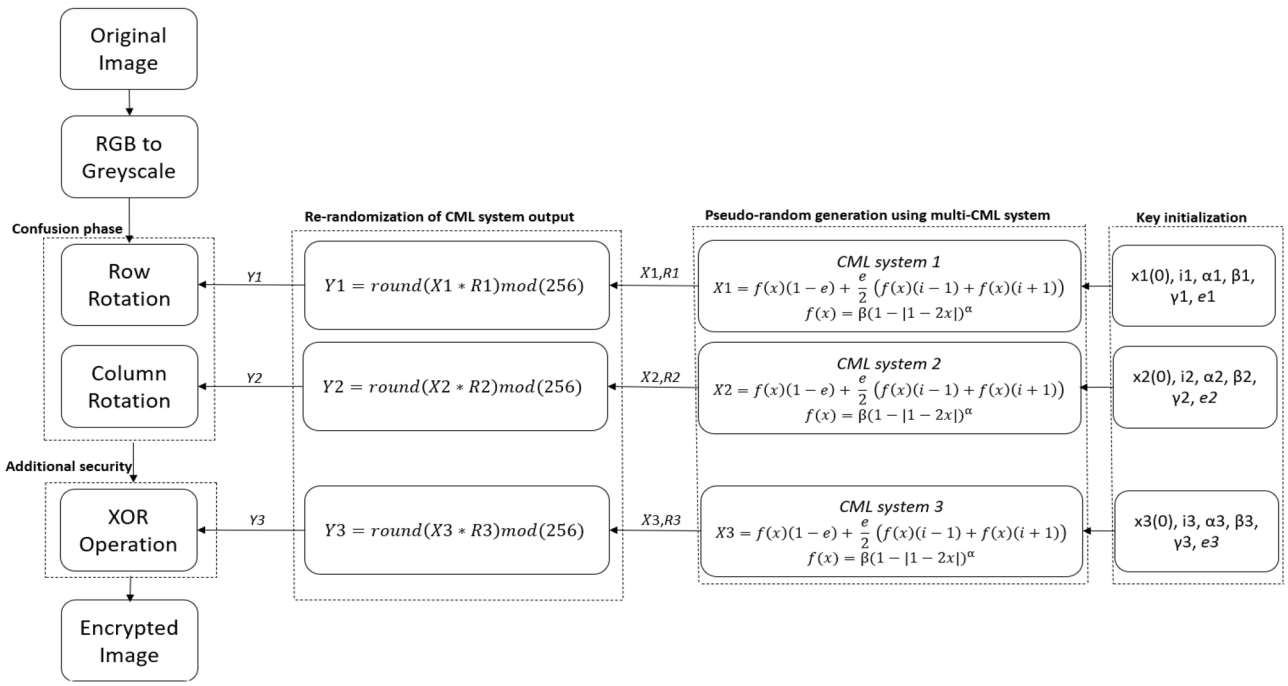

Fig. 11 Architecture of the proposed image encryption system

- The confusion phase scrambles the image pixels to make the image unrecognizable.
- The pseudo-random sequence $Y1$ is used for arow rotation process.
- If the random sequence value for $Y1$ is even, the corresponding pixel $P(x, y)$ moves $Y1$ spaces to the left of present pixel position, i.e., $P(x - Y1, y)$. Whereas, if the sequence value for $Y1$ is odd, the pixel is moved $Y1$ spaces to the right with respect to the present pixel position, i.e., $P(x + Y1, y)$.
- The pseudo-random sequence $Y2$ is used for column rotation process.
- If the random sequence value for $Y2$ is even, the corresponding pixel $P(x, y)$ moves $Y1$ spaces to the top of present pixel position $P(x, y + Y2)$. Whereas, if the sequence value for $Y2$ is odd, the pixel is moved $Y2$ spaces to the bottom with respect to the present pixel position $P(x, y - Y2)$.

STEP 6: Additional security

- XOR operator has a special characteristic that makes it suitable for in cryptography, it is irreversible without the knowledge of key it was used to XOR with.
- Each image pixel of the shuffled image from Step 5 is XORed with pseudo-random sequence $Y3$.
- Confusion phase scrambles the location of image pixels, whereas XOR operation changes the value of image pixel to some other value that has no relation to the original image.

The completion of the above six steps leads to the generation of a cipher image which cannot be recognized visually as well as statistically. Figure 12 shows an illustration of image encryption for a publicly available image (boat.jpg) of size 512×512 pixels. All the images used for experiments in this paper have been taken from publicly available image datasets by University of Southern California [57] and University of Waterloo [58]. The parameters used as keys for the encryption process are as follows: $x1(0) = 0.2563$, $x2(0) = 0.3765$, $x3(0) = 0.7452$, $\alpha 1 = 0.7$, $\alpha 2 = 1.1$, $\alpha 3 = 2.5$, $\beta 1 = \beta 2 = \beta 3 =$ adaptive, $\gamma 1 = 0.250$, $\gamma 2 = 0.150$, $\gamma 3 = 0.250$, $\epsilon 1 = 0.8$, $\epsilon 2 = 0.5$, $\epsilon 3 = 0.4$, $i = 10$, $R1 = 5 \times 10^5$, $R2 = 2 \times 105$, $R3 = 3 \times 105$. The number of iterations was set to 7×10^4 for the CML system [Eq. (1)]. Figure 12a and b shows the original image and its histogram, whereas Fig.12c and d represents the cipher image and its histogram. It can be seen from the figure that the histogram of the cipher image shows no information that could match to the original image histogram.

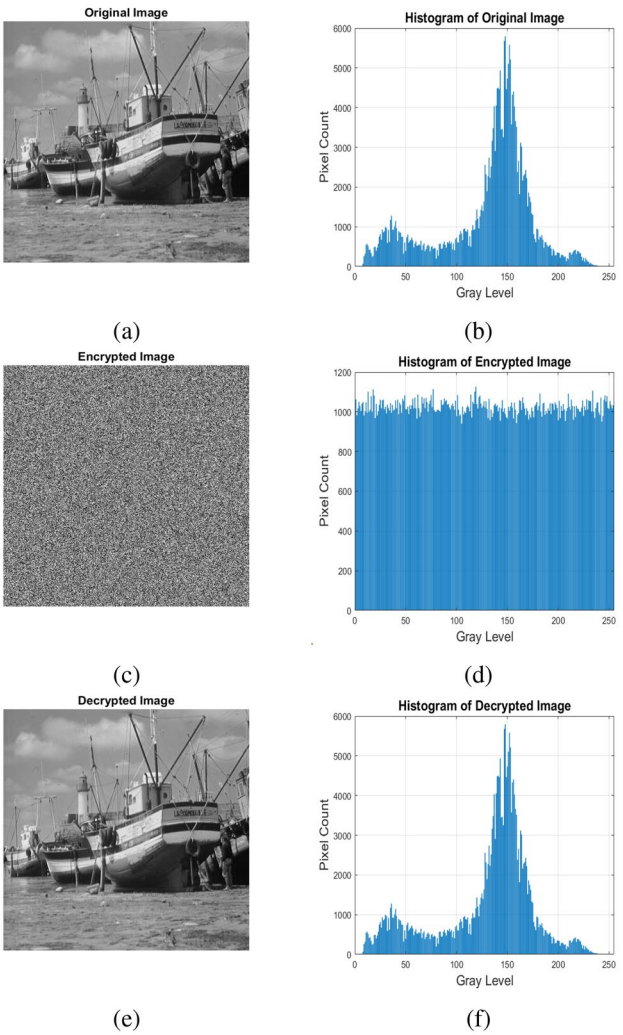

Fig. 12 Illustration of image encryption and decryption process applied on boat image (image size = 512×512)

Decryption Process

The decryption method is exactly the reverse procedure as the encryption process. The six steps shown in the encryption process are repeated with the same parameters and keys used for encryption of the image. The bottom row of Fig. 12e shows the decrypted image and (f) is the histogram plot. The information can be matched with the original image and its histogram also shown in Fig. 12 (top row), the recovered image (bottom row) is exactly the same as the original image.

Histogram Analysis

Some chaos-based image encryption schemes can generate an encrypted image that visually does not look like the original image, but with a few statistical tests, the original image

can be recovered from original image [59–61]. Histogram analysis is a universally used statistical method to look out for the image signal details. For fair testing of the proposed algorithm, we choose images of different sizes and colors (grayscale and RGB) to be verified with histogram equalization scheme. Figure 13 shows the results of the experiments performed on four images with different characteristics (size and color). Figure 13a is the histogram plotted for the grayscale lena image of size 256×256, and (b) shows the histogram of same image after proposed encryption scheme was applied on it. Figure 13c is the histogram for the grayscale cameraman image of size 256×256, and (d) shows the histogram of the encrypted cameraman image.

Figure 13e is the histogram for the colored baboon image of size 512×512, and (f) shows the histogram of the encrypted baboon image. It can be clearly observed that despite the different type of image samples used, the encrypted images do not reveal any information that could relate to original images as the histograms of encrypted images show even distribution of grayscale levels.

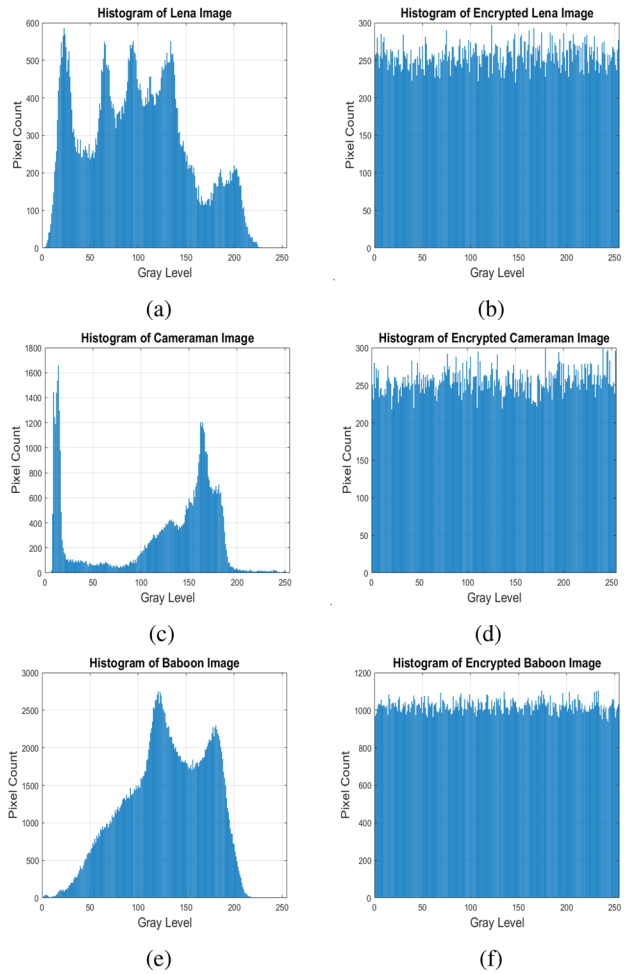

Fig. 13 Histograms of original images and encrypted images

Key Ssensitivity Testing

Testing the cryptosystem against key sensitivity is one of the most important tests, as it determines the security level of the system. Cryptosystems with higher sensitivity to keys are considered suitable for encryption purposes, as they do not allow the data to be decrypted if there is a slight change made to the encryption key. Table 2 shows two types of keys used for key sensitivity analysis. $KEY1$ (original) is the key that was used to encrypt the original image, whereas $KEY2$ (corrupted) is assumed as a corrupted version of key that an attacker might use.

The top row of Fig. 14 shows the lena image that was encrypted using $KEY1$ and its histogram, while the bottom row shows the image decrypted using $KEY2$ and its histogram. This can be deduced from the tests that even if a minor change as small as 1×10^{-15} is made to the key, then the proposed cryptosystem would not accept it as the decryption key and will fail the decryption process.

Key Space Analysis

The key space of a cryptosystem is considered a factor to categorize the robustness of a cryptosystem towards brute force attacks. There are no criteria of an ideal key space, but a key space should at least be 2^{100} to resist brute force attacks [62]. There are a total of 19 initial conditions and control parameters that serve as the encryption key for the proposed system ($x1$, $x2$, $x3$, $\alpha1$, $\alpha2$, $\alpha3$, $\beta1$, $\beta2$, $\beta3$, $\gamma1$, $\gamma2$, $\gamma3$, $\epsilon1$, $\epsilon2$, $\epsilon3$, i, $R1$, $R2$, $R3$). The experiments for the implementation of the proposed system were performed

Table 2 Two different versions of keys used for key sensitivity testing

$KEY1$ (original)	$KEY2$ (corrupted)
$x1(0) = 0.2563$	$x1(0) = 0.2563 + 1 \times 10^{-15}$
$x2(0) = 0.3765$	$x2(0) = 0.3765 + 1 \times 10^{-15}$
$x3(0) = 0.7452$	$x3(0) = 0.7452 + 1 \times 10^{-15}$
$\alpha1 = 0.7$	$\alpha1 = 0.7$
$\alpha2 = 1.1$	$\alpha2 = 1.1$
$\alpha3 = 2.5$	$\alpha3 = 2.5$
$\beta1 = \beta2 = \beta3 =$ adaptive	$\beta1 = \beta2 = \beta3 =$ adaptive
$\gamma1 = 0.250$	$\gamma1 = 0.250$
$\gamma2 = 0.150$	$\gamma2 = 0.150$
$\gamma3 = 0.250$	$\gamma3 = 0.250$
$\epsilon1 = 0.8$	$\epsilon1 = 0.8$
$\epsilon2 = 0.5$	$\epsilon2 = 0.5$
$\epsilon3 = 0.4$	$\epsilon3 = 0.4$
$R1 = 5 \times 10^5$	$R1 = 5 \times 10^5$
$R2 = 2 \times 10^5$	$R2 = 2 \times 10^5$
$R3 = 3 \times 10^5$	$R3 = 3 \times 10^5$
$i = 10$	$i = 10$

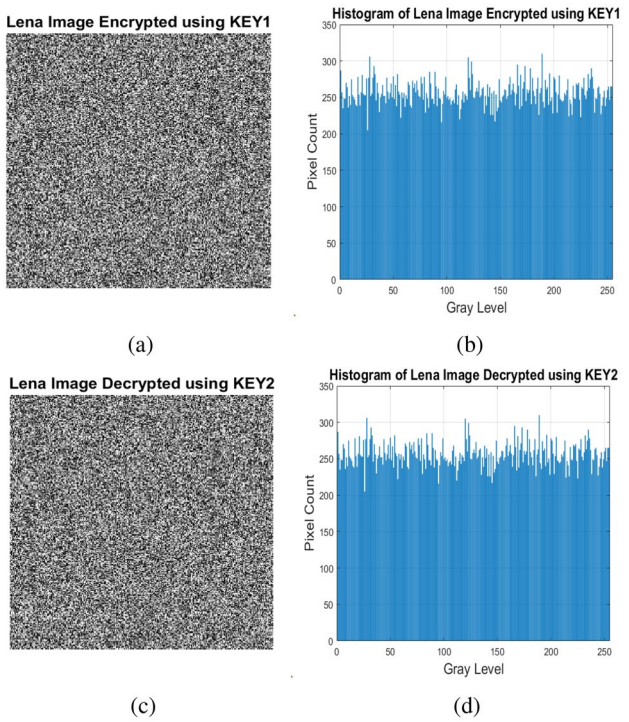

Fig. 14 Image encrypted using *KEY*1 and its histogram (top row), and image decrypted using *KEY*2 and its histogram (bottom row)

Table 3 Comparison of few other image encryption algorithms based on CML and their key space values with the proposed method

Algorithm	Key space
LDCML [29]	2^{480}
2D NACML [32]	–
MLNCML [33]	2^{400}
Chaos-DNA [37]	2^{256}
LSSCML [38]	2^{249}
MCML [45]	2^{400}
Proposed method	2^{850}

using MATLAB R2021, which uses the IEEE standard 754 for double precision variables represented by 64 bits in 16 digits (10^{-16}). To calculate the key space, we assume that the 16 key variables ($x1$, $x2$, $x3$, $\alpha1$, $\alpha2$, $\alpha3$, $\beta1$, $\beta2$, $\beta3$, $\gamma1$, $\gamma2$, $\gamma3$, $\epsilon1$, $\epsilon2$, $\epsilon3$, i) were presented using double precision which is 16 digits: $(10^{16})^{16} = 10^{256}$. The remaining three key variables ($R1$, $R2$, $R3$) were presented using precision (10^{-15}); therefore, its key space can be calculated as: $(10^{15})^3 = 10^{45}$. Hence, the total key space of the proposed system can be calculated as: $10^{240} * 10^{45} \cong 10^{285} \cong 2^{850}$. The key space of the proposed system has been compared with existing CML-based image encryption algorithms. Table 3 shows results of the comparison, which concludes that the key space of proposed method is the highest compared to other existing algorithms.

Table 4 Information entropy analysis for a few sample images and their encrypted versions using the proposed image encryption scheme

Image used for IE	Original image	Encrypted image
Lena	7.5694	7.9895
Baboon	7.3589	7.9916
Peppers	7.5945	7.9912
Cameraman	7.0148	7.9897

Table 5 Information entropy comparison between proposed method results and existing CML-based image encryption algorithms tested on Lena image

Algorithm	Information entropy
LDCML [29]	7.9023
2D NACML [32]	7.9971
MLNCML [33]	–
Chaos-DNA [37]	7.9993
LSSCML [38]	7.9975
MCML [45]	7.9993
Proposed method	7.9895

Information Entropy

The principles of ergodicity and confusion in chaotic systems claim that in a chaotic system, the values generated during each iteration must be distributed uniformly in the range [0,1]. Therefore, for chaotic systems, the degree of chaos can be quantified using of information entropy. The less ordered a system, the higher the information entropy of the system. Shannon proposed the idea of information entropy in 1948 which could be calculated as shown in Eq. (7) [63]

$$H(s) = -\sum_{1}^{n} (P(s_i) \times \log_2 P(s_i)), \tag{7}$$

where s represents the information source and $P(s_i)$ is the probability of the source s_i and n shows the length of the sequence. Theoretically, the ideal value of information entropy for a true random source s should be $H(s) = 8$. In case of image encryption, the encrypted image should possess information entropy closes to this ideal value. Table 4 shows the information entropy analysis for few famous images and also their encrypted versions. This could be deduced from Table 3 that the encrypted versions of images have entropy values higher than 7.9 which means that they are quite robust to attacks. Table 5 shows further comparison of the proposed algorithm with existing image encryption algorithms based on CMLs.

Correlation Coefficient Analysis

In an image, the pixels are correlated to collectively display image information, but for an encrypted image, the pixels should reflect weak correlation. Image encryption algorithms that exhibit small correlation amongst the pixels are considered better techniques. Correlation coefficients can be calculated using the equations below

$$E(X) = \frac{1}{n}\sum_{i=1}^{n} x_i, \tag{8}$$

$$V(X) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(X))^2, \tag{9}$$

$$\text{cov}(X, Y) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(X))(y_i - E(Y)), \tag{10}$$

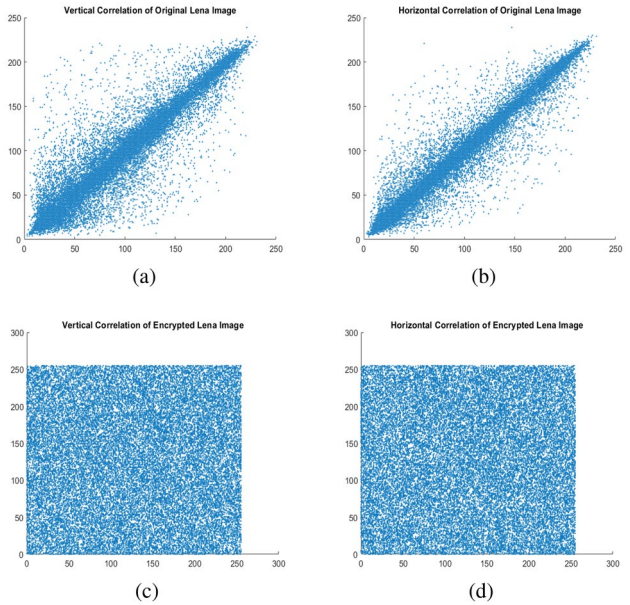

Fig. 15 Correlation between vertical and horizontal pixels of original lena image (top row) and encrypted lena image (bottom row)

$$R(X, Y) = \frac{\text{cov}(X, Y)}{\sqrt{V(X)V(Y)}}, \tag{11}$$

where $X = \{x_1, ..., x_n\}$ represents a set of randomly chosen pixels from the image, and $Y = \{y_1, ..., y_m\}$ denotes adjacent pixels to X. In a two-dimensional image, for vertical correlation, the adjacent pixel would be above or below pixels, whereas for horizontal correlation, the adjacent pixel would be from either side of the chosen pixel. Figure 15 shows plots of horizontal and vertical correlation between the original and ciphered image Lena of size 256×256. It can be clearly observed from the plots that for the original lena image, the pixel intensities correlates. While for the encrypted image, pixels are evenly distributed across x and y axis, exhibiting no correlation.

Table 6 shows horizontal and vertical correlation values for a few sample images and their encrypted versions. In the original images the correlation values are high, meaning that the pixels are closely related. Whereas, in case of the encrypted images, the correlation values are close to zero which means that there exists no correlation between the images. The encryption was performed using the proposed method. Table 7 shows another comparison of proposed method and existing image encryption techniques in terms of correlation coefficients.

Differential Attack Analysis

Another important test for an image encryption algorithm is to test it against differential attack. Crypt-analysts are mostly interested in attacking weak encryption algorithms, such as

Table 7 Correlation coefficients' comparison between the proposed method and existing techniques tested on lena image

Algorithms	Original image		Encrypted image	
	Horizontal	Vertical	Horizontal	Vertical
LDCML [29]	0.9772	0.9856	0.0003	0.0023
2D NACML [32]	0.9655	0.9379	0.0406	0.0378
MLNCML [33]	0.9696	0.9876	0.0013	− 0.0002
Chaos-DNA [37]	0.9794	0.9646	0.0214	0.0465
LSSCML [38]	0.9688	0.9376	− 0.0077	0.0002
MCML [45]	0.9722	0.9856	− 0.0005	− 0.0036
Proposed method	0.8942	0.9696	− 0.0124	− 0.0013

Table 6 Horizontal and vertical correlation values for different sample images

Image coefficients	Lena		Baboon		Peppers		Cameraman	
	Original	Encrypted	Original	Encrypted	Original	Encrypted	Original	Encrypted
Horizontal	0.8942	− 0.0124	0.8572	0.0036	0.9419	− 0.0015	0.9813	− 0.0135
Vertical	0.9696	− 0.0013	0.7495	− 0.0007	0.9761	− 0.0020	0.9584	− 0.0004

Table 8 UACI (%) and NPCR (%) calculations for few sample images

Image coefficients	Lena	Baboon	Peppers	Cameraman
UACI (%)	33.49	33.42	33.51	33.48
NPCR (%)	99.57	99.59	99.60	99.60

Table 9 UACI (%) and NPCR (%) comparison of proposed method with existing algorithms tested on lena image

Algorithms	UACI (%)	NPCR (%)
LDCML [29]	33.41	99.61
2D NACML [32]	33.40	99.59
MLNCML [33]	33.50	99.78
Chaos-DNA [37]	33.51	99.61
LSSCML [38]	33.47	99.60
MCML [45]	33.39	99.63
Proposed method	33.49	99.60

algorithms insensitive to change in pixel values. A common strategy opted by attackers is to make slight change in pixel values and observe the change in encrypted image. Unified Average Changing Intensity (UACI) and Number of Pixel Change Rate (NPCR) are two checks that can be applied to measure sensitivity of an encryption algorithm to differential attacks. UACI and NPCR can be calculated as shown in the following equations:

$$D(i,j) = \begin{cases} 1 & \text{if} \quad c_1(i,j) \neq c_2(i,j) \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

$$\text{NPCR} = \frac{1}{MN}\left(\sum_{i,j} D(i,j)\right) \tag{13}$$

$$\text{UACI} = \frac{1}{MN}\left[\sum_{i,j} \frac{c_1(i,j) - c_2(i,j)}{255}\right]. \tag{14}$$

In the above equations, $c1$ and $c2$ are two cipher images with slight change in values and $M \times N$ is the size of cipher image. Table 8 shows UACI (%) and NPCR (%) calculations using the proposed method for a few sample images. The results show the least value of UACI for different images is 33.42% and NPCR is 99.57% but are still sufficient to maintain integrity of the encrypted images. Table 9 shows a comparison of UACI and NPCR values generated using the proposed method and existing state-of-the-art methods.

Conclusion

In this paper, a novel CML system is used to generate seed values for an image encryption algorithm. The CML system uses generalised symmetric maps and adaptive β values, which contribute towards a larger key space and makes it more likely the system remains in chaos for the input values. Considering the need of strong cryptographic schemes for image encryption, a multi-coupled map lattice system is proposed to encrypt and decrypt images. The proposed cryptosystem has been thoroughly tested using statistical analysis, key sensitivity experiments, information entropy comparison, correlation coefficient analysis, and differential attack testing. The results provide strong evidence that the proposed system is robust towards the majority of attacks, such as brute force and plain-text attack, etc. A comparative analysis was also performed between the proposed technique and existing state-of-the-art CML-based image encryption methods and the results show that the proposed algorithm performs better than most of the existing solutions. Therefore, the conclusion can be drawn based on the comprehensive testing and fair analysis that the proposed solution is suitable for images of any type and size. The shortcoming of the proposed algorithm is that it is not suitable for highly resource constrained devices, as it depends on three iterative CML systems which requires computational resources to calculate pseudo-random sequences. Future work includes optimization of the proposed system for devices with low computational power.

Funding This research is supported by the BTIIC (British Telecom Ireland Innovation Centre) project, funded by British Telecom and Invest Northern Ireland.

Declarations

Conflict of Interest The authors have no conflicts of interest to declare. All co-authors have seen and agreed with the contents of the manuscript. We certify that the submission is original work and is not under review at any other publication.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Lorenz EN. Deterministic nonperiodic flow. J Atmos Sci. 1963;20(2):130–41.
2. Kocarev L, Lian S. Chaos-based cryptography: theory, algorithms and applications, vol. 354. Berlin: Springer Science & Business Media; 2011.
3. Ivancevic VG, Ivancevic TT. High-dimensional chaotic and attractor systems: a comprehensive introduction, vol. 32. Berlin: Springer Science & Business Media; 2007.
4. Zia U, McCartney M, Scotney B et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int J Inf Secur. 2022;21:917–35. https://doi.org/10.1007/s10207-022-00588-5.
5. Oono Y, Shiwa Y. Computationally efficient modeling of block copolymer and benard pattern formations. Mod Phys Lett B. 1987;1(01n02):49–55.
6. Kessler DA, Levine H, Reynolds WN. Coupled-map lattice model for crystal growth. Phys Rev A. 1990;42(10):6125.
7. Pandit R, Pande A, Sinha S, Sen A. Spiral turbulence and spatiotemporal chaos: characterization and control in two excitable media. Phys A Stat Mech Appl. 2002;306:211–9.
8. Yanagita T. Phenomenology of boiling: a coupled map lattice model. Chaos Interdiscip J Nonlinear Sci. 1992;2(3):343–50.
9. Yanagita T, Kaneko K. Coupled map lattice model for convection. Phys Lett A. 1993;175(6):415–20.
10. Yanagita T, Kaneko K. Modeling and characterization of cloud dynamics. Phys Rev Lett. 1997;78(22):4297.
11. Nishimori H, Ouchi N. Formation of ripple patterns and dunes by wind-blown sand. Phys Rev Lett. 1993;71(1):197.
12. Ito H, Glass L. Spiral breakup in a new model of discrete excitable media. Phys Rev Lett. 1991;66(5):671.
13. Beck C. Spatio-temporal chaos and vacuum fluctuations of quantized fields, vol. 21. Singapore: World Scientific; 2002.
14. Kaneko K. Overview of coupled map lattices. Chaos Interdiscip J Nonlinear Sci. 1992;2(3):279–82.
15. Huang R, Han F, Liao X, Wang Z, Dong A. A novel intermittent jumping coupled map lattice based on multiple chaotic maps. Appl Sci. 2021;11(9):3797.
16. Khellat F, Ghaderi A, Vasegh N. Li-yorke chaos and synchronous chaos in a globally nonlocal coupled map lattice. Chaos Solitons Fractals. 2011;44(11):934–9.
17. Meherzi S, Marcos S, Belghith S. A new spatiotemporal chaotic system with advantageous synchronization and unpredictability features. In: Proc. Nolta. 2006.
18. You-Ming Y, Jian-Dong L. A tcml-based spatiotemporal chaotic one-way hash function with changeable-parameter. Acta Phys Sin. 2007;56(3):1297–304.
19. Sinha S. Random coupling of chaotic maps leads to spatiotemporal synchronization. Phys Rev E. 2002;66(1):016–209.
20. Rajesh S, Sinha S, Sinha S. Synchronization in coupled cells with activator-inhibitor pathways. Phys Rev E. 2007;75(1):011–906.
21. Mondal A, Sinha S, Kurths J. Rapidly switched random links enhance spatiotemporal regularity. Phys Rev E. 2008;78(6):066–209.
22. Poria S, Shrimali MD, Sinha S. Enhancement of spatiotemporal regularity in an optimal window of random coupling. Phys Rev E. 2008;78(3):035–201.
23. Chen Y, Xiao J, Wu Y, Li L, Yang Y. Optimal windows of rewiring period in randomly coupled chaotic maps. Phys Lett A. 2010;374(31–32):3185–9.
24. Zhang YQ, Wang XY. Spatiotemporal chaos in mixed linear-nonlinear coupled logistic map lattice. Phys Stat Mech Appl. 2014;402:104–18.
25. Zhang YQ, Wang XY. Spatiotemporal chaos in arnold coupled logistic map lattice. Nonlinear Anal Model Control. 2013;18(4):526–41.
26. Kaneko K. Spatiotemporal chaos in one-and two-dimensional coupled map lattices. Phys Nonlinear Phenom. 1989;37(1–3):60–82.
27. Muruganandam P, Francisco G, de Menezes M, Ferreira FF. Low dimensional behavior in three-dimensional coupled map lattices. Chaos Solitons Fractals. 2009;41(2):997–1004.
28. Zhang L, Liu S, Yu C. Chaotic behaviour of nonlinear coupled reaction-diffusion system in four-dimensional space. Pramana. 2014;82(6):995–1009.
29. Xingyuan W, Le F, Shibing W, Zhang C, Yingqian Z. Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access. 2018;6:39(724):705–39.
30. Ausloos M. The logistic map and the route to chaos: From the beginnings to modern applications. Berlin: Springer Science & Business Media; 2006.
31. Hao Z, Xing-yuan W, Si-wei W, Kang G, Xiao-hui L. Application of coupled map lattice with parameter q in image encryption. Opt Lasers Eng. 2017;88:65–74.
32. Yj S, Zhang H, Xy W, Xq W, Pf Y. 2d non-adjacent coupled map lattice with q and its applications in image encryption. Appl Math Comput. 2020;373(125):039.
33. Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci. 2014;273:329–51.
34. Zhang YQ, Wang XY, Liu J, Chi ZL. An image encryption scheme based on the MLNCML system using DNA sequences. Opt Lasers Eng. 2016;82:95–103.
35. Li X, Zhou C, Xu N. A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos. Int J Netw Secur. 2018;20(1):110–20.
36. Song C, Qiao Y. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy. 2015;17(10):6954–68.
37. Zhen P, Zhao G, Min L, Jin X. Chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl. 2016;75(11):6303–19.
38. Hu T, Liu Y, Gong LH, Guo SF, Yuan HM. Chaotic image cryptosystem using DNA deletion and DNA insertion. Signal Process. 2017;134:234–43.
39. Fu XQ, Liu BC, Xie YY, Li W, Liu Y. Image encryption-then-transmission using DNA encryption algorithm and the double chaos. IEEE Photonics J. 2018;10(3):1–15.
40. Xy W, Hl Z, Xm B. Color image encryption scheme using CML and DNA sequence operations. Biosystems. 2016;144:18–26.
41. Wu X, Wang K, Wang X, Kan H, Kurths J. Color image DNA encryption using NCA map-based cml and one-time keys. Signal Process. 2018;148:272–87.
42. Wang X, Qin X, Liu C. Color image encryption algorithm based on customized globally coupled map lattices. Multimed Tools Appl. 2019;78(5):6191–209.
43. Nematzadeh H, Enayatifar R, Motameni H, Guimarães FG, Coelho VN. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng. 2018;110:24–32.

44. Wang X, Feng L, Li R, Zhang F. A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. Nonlinear Dyn. 2019;95(4):2797–824.
45. Wang X, Zhao H, Wang M. A new image encryption algorithm with nonlinear-diffusion based on multiple coupled map lattices. Opt Laser Technol. 2019;115:42–57.
46. Oravec J, Turan J, Ovsenik L. Image encryption technique with key diffused by coupled map lattice. In: 2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA). IEEE; 2018. p. 1–6.
47. Wu X, Li Y, Kurths J. A new color image encryption scheme using cml and a fractional-order chaotic system. PLoS One. 2015;10(3):e0119660.
48. Liu Q, Py L, Mc Z, Yx S, Hj Y. A novel image encryption algorithm based on chaos maps with Markov properties. Commun Nonlinear Sci Numer Simul. 2015;20(2):506–15.
49. Zia U, McCartney M, Scotney B, Martinez J, Sajjad A. A novel pseudo-random number generator for iot based on a coupled map lattice system using the generalised symmetric map. SN Appl Sci. 2022;4(2):1–17.
50. Kaneko K. Coupled Map Lattice. In: Artuso R, Cvitanović P, Casati G, editors. Chaos, Order, and Patterns. NATO ASI Series, vol. 280. Boston, MA: Springer; 1991. https://doi.org/10.1007/978-1-4757-0172-2_10.
51. Kaneko K. Pattern dynamics in spatiotemporal chaos: pattern selection, diffusion of defect and pattern competition intermettency. Phys D Nonlinear Phenom. 1989;34(1–2):1–41.
52. Markus M, Hess B. Chapter 12 - Lyapunov exponents of the logistic map with periodic forcing, In: Clifford A, editor. Pickover, Chaos and Fractals, Elsevier Science; 1998, pp. 73–8. https://doi.org/10.1016/B978-044450002-1/50015-1.
53. Shibata H. Ks entropy and mean lyapunov exponent for coupled map lattices. Phys A Stat Mech Appl. 2001;292(1–4):182–92.
54. Just W. Bifurcations in globally coupled map lattices. J Stat Phys. 1995;79(1):429–49.
55. Kaneko K. Lyapunov analysis and information flow in coupled map lattices. Phys D Nonlinear Phenom. 1986;23(1–3):436–47.
56. Mao Y, Chen G. Chaos-based image encryption. In: Handbook of geometric computing. Springer; 2005. p. 231–265.
57. Weber A. The USC-SIPI image database. 2018. https://sipi.usc.edu/database/. Accessed 30 Sept 2021.
58. Set WG University of waterloo fractal coding and analysis group: Mayer gregory image repository. Source: 2009. http://linksuwaterlooca/Repositoryhtml.
59. Zhang X, Nie W, Ma Y, Tian Q. Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic s-box. Multimed Tools Appl. 2017;76(14):15,641-15,659.
60. Li S, Zheng X. Cryptanalysis of a chaotic image encryption method. In: 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353), vol. 2. IEEE; 2002. p. II.
61. Jeng FG, Huang WL, Chen TH. Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. Signal Process Image Commun. 2015;34:45–51.
62. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos. 2006;16(08):2129–51.
63. Caves CM. Information, entropy, and chaos. Physical Origins of Time Asymmetry. 1994; p. 47–89.