A New Hybrid Image Encryption Technique using Lorenz Chaotic System and Simulated Kalman Filter (SKF) Algorithm

Nurnajmin Qasrina Ann[1], Dwi Pebrianti[1], Mohd Fadhil Abas[2], Luhur Bayuaji[3]

[1] College of Engineering, Universiti Malaysia Pahang, Gambang Malaysia
[2] Faculty of Electrical and Electronics Engineering Technology, Universiti Malaysia Pahang, Pekan Malaysia
3 Faculty of Computing, Universiti Malaysia Pahang, Pekan Malaysia
qasrinaann@gmail.com

Abstract. Nowadays, encryption is one of the most popular and effective security methods used by company and organizations. A new hybrid technique, Lorenz chaotic system and an optimization algorithm, Simulated Kalman Filter (SKF) had been proposed to solve image encryption problem. The objectives of the hybrid technique are to improve the security and add noise from the optimization algorithm and generate chaotic secret key. To achieve that, Lorenz chaotic system is implemented to this method and produce secret key sequence. SKF is one of the optimization methods that had been proved to have great performance in engineering applications from prediction, measurement, and estimation process. Thus, the proposed method is outperformed the results and analysis compared to literature as benchmarks. In short, the proposed hybrid approach is agile and efficient to apply in image encryption problem.

Keywords: Image encryption, Lorenz chaotic system, Correlation.

1 Introduction

Chaotic system is a dynamical system appear in random states of disorder and irregularities that is sensitive to initial conditions. Due to this system is characterized to be deterministic and complex, it is suitable for image encryption application. Today, encryption is one of the most common and efficient methods of security used by companies and organizations. Picture encryption transforms images with a unique secret key, also called the decryption key, into another type of code. Image encryption is intended to secure the security of digital data when it is stored on computer systems and distributed over the internet or other computer networks. The image encryption algorithms usually provide anonymity and drive key protection measures such as authentication, honesty, and non-reputation. The most basic form of attacking encryption is brute-force or attempting random keys before you find the correct one.

Because of its numerous applications in population dynamics, electrical circuits, cryptology, fluid dynamics, engineering, stock markets, etc., several researchers have studied chaotic systems extensively. For example, in fluid dynamics, the chaotic characteristic is in turbulence which is the changes in pressure and flow velocity. Chaos theory suggests investors to research about the effect and probability theories and outcomes to predict market activity. The chaotic and hyperchaotic system of nonlinear ordinary differential equations (ODEs) is characterized by the dynamical phenomena. In the literature, much study has been documented investigating different types of characteristics associated with dynamical systems [1]. In addition, the authors mainly researches the feature point set's chaotic character, generated by iterating the image and the auxiliary surface [2]. The study found that images could be identified by the feature point collection, which concerns a chaotic attractor. The feature point set is expected to become a major feature in the fields of target detection and image recognition. The extraction of image feature point sets based on the iteration has some parallels compared to the artificial neural network. In this technique, images are iterating functions or weight values. This technique is not contrary to the mechanism of vision, and it may be one of the mechanisms of memory thought and revival.

Cryptography is secret to the original data by converting it to cipher data to ensuring retrieve this data on the receiver side without losing some data or deformation the resolution. Image encryption is a technique which coding the original image (plain image) to another un-understanding image (cipher image). This technique must be providing the decoding of the cipher image to plain image without losing data or image properties [3]. Many encryption algorithms use to protect and ciphered text data, such as classical cipher systems. There are Hill Cipher System, Arnold Cat Map System, and Vigener Cipher. The chaotic cryptography becomes an important research topic in chaos nowadays. Chai et al. introduced the architecture of permutation and diffusion based on the chaotic system into medical images [4]. There is a higher correlation between adjacent pixels in medical images compared to natural images, and therefore the successful pixel permutation method must be generated to eliminate the correlation. A convincing form of image encryption must have the capacity to encrypt plain images into unrecognized cipher images, and only with the correct key can the cipher image be absolutely decrypted.

With the advent of the Internet age, much of the data in existence cannot be isolated from the assistance of the Internet. The authors implement an image encryption algorithm based on the memristive chaotic system, elementary cellular automata, and compressive sensing in order to ensure information security. [5]. The zigzag path and elementary cellular automata scramble the wavelet coefficients of the plain image. A circular measurement matrix formed by a new kind of magnetic regulated memristive chaotic system is adopted for compressive sensing, further decreasing the energy consumption of data transmission. To get some parameters used in the encryption process, the SHA-512 hash value of the original image uses the algorithm to have a high relationship with the plain image. Today, the number of publicly distributed digital images and shared networks continues to grow. An image segmentation encryption algorithm based on the chaotic hybrid framework is suggested in this review. [6]. The chaotic pointer created by another Quantum Cellular Neural Network and a chaotic 3-D system is viewed from the essential pool as indexes to get keys for image segmentation, pixel exchange rule, scrambling, and diffusion. The 4-D hyper-chaotic method was used to scramble the sequence of the Quantum Cellular Neural Network to produce the quantum.

On the other hand, an approach is suggested in [7] for encrypting images using Particle Swarm Optimization (PSO) and chaotic logistic map. In this paper, PSO is implemented to look for the optimal encrypted image in which the optimization aims to minimize the association between adjacent image pixels. Then, using the Genetic Algorithm (GA) and Lorenz chaotic method, the hybrid image encryption technique was proposed in [8]. The goal of the authors is to propose an integrated algorithm that utilizes chaotic systems' agility, efficiency and high key sensitivity, and the genetic algorithm's optimizing capacity.

In this research, a hybrid technique for image encryption application using Simulated Kalman Filter (SKF) and Lorenz chaotic system is proposed. The Lorenz chaotic system is used to generate the secret key and the systems is no doubt due to their excellent performance in generating highly sensitive keys and prompt result. The optimization algorithm SKF has an important role to search the optimal encrypted image based on the fitness function such correlation.

The rest of the paper: Section 1 is about to introduce the background study and some literature reviews. Then, Section 2 explained about the proposed methodology in this study which are divided into three parts. Subsequently, Section 3 is discussed about results and four analysis to proof either the proposed method is suitable for image encryption or not. Lastly, the study is concluded in Section 4.

2 Methodology

This section is divided into three parts which are the first two parts are encryption process and the third part is decryption process. The encryption process consists of two stages. The first stage is encryption process with Lorenz chaotic system while the second stage is encryption process with Simulated Kalman Filter (SKF) algorithm. The methodology of the study is summarized in Fig. 1 below.

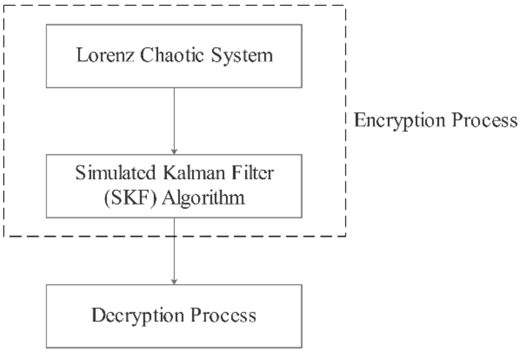


Fig. 1. Project Flowchart

2.1 Encryption Process with Lorenz Chaotic System

Because of their excellent success in producing susceptible keys and the speed at which they produce results, chaos-based cryptographic systems have become an important part of data encryption techniques [8]. Encryption is the process of converting data into a different format or code that can only be accessed by anyone with a decryption key or password. Image sharing had become a major part of people's daily lives as computer networks grew in popularity. The value of privacy cannot be overstated.

Fig. 2 is the flowchart of the encryption process for the Lorenz chaotic system. The flowchart is summarized on how Lorenz system approach can generate the random sequence for encrypted purposed.

$$\begin{aligned} \dot{x} &= \frac{dx}{dt} = a(y - x), \\ \dot{y} &= \frac{dy}{dt} = cx - y - xz, \\ \dot{z} &= \frac{dz}{dt} = xy - bz. \end{aligned} \tag{1}$$

The proposed image encryption algorithm is summarized in the flowchart below. From equation (1), the real number given by α, r and b are the control parameters. In contrast, real values are given by x, y and z are called the state variables, and the equations itself are for the time derivatives of the variables x, y and z. For a given set of control parameters and the initial set of values x_0, y_0 and z_0 which are the initial state variables are provided. These values are seed values combined with a set called the seed set, the encryption and decryption key for this method. The system is non-linear and non-periodic, which means its values do not repeat over time, and it takes three input variables: x, y and z. This denotes a three-dimensional and deterministic structure. As a result, from a given current state and inputs, the next state can always be predicted.

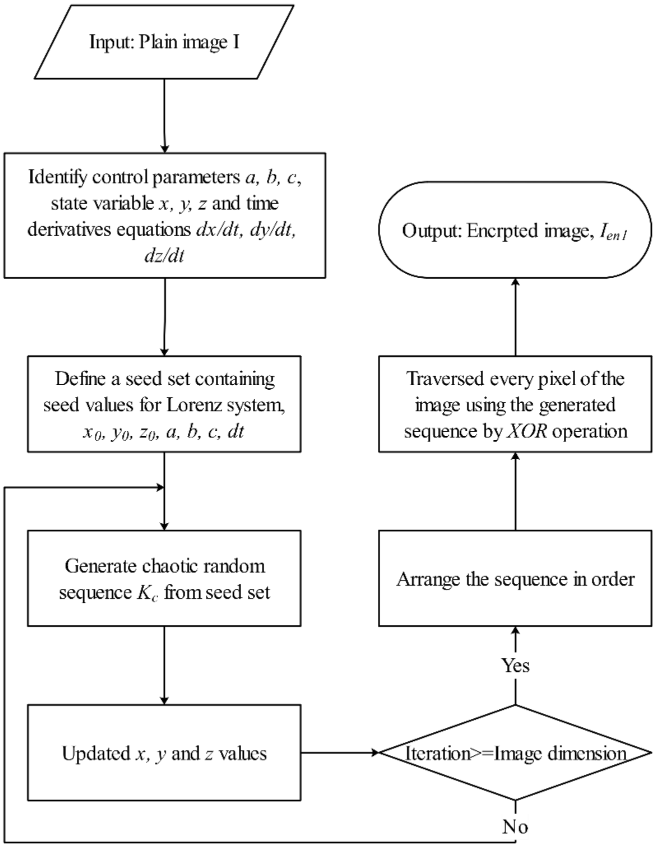

Input: Plain image I
Identify control parameters *a, b, c*, state variable *x, y, z* and time derivatives equations *dx/dt, dy/dt, dz/dt*
Define a seed set containing seed values for Lorenz system, $x_0, y_0, z_0, a, b, c, dt$
Generate chaotic random sequence K_c from seed set
Updated *x, y* and *z* values
Iteration>=Image dimension
Yes
No
Arrange the sequence in order
Traversed every pixel of the image using the generated sequence by *XOR* operation
Output: Encrpted image, $I_{en\,I}$

Fig. 2. Image Encryption Algorithm (First Stage)

The first step is the random sequence generation by defining a key or seed set containing the Lorenz system's seed values. The x_0, y_0 and z_0 values are taken from [9] that consist of a very high-precision numerical and validated initial conditions of periodic orbits for the Lorenz model. Instead of random values, the data can be used as a harsh test for modern computational and analytical techniques aimed at unpredictable dissipative systems. After that, for control parameters, the values a, b and c chosen are 10, $8/3$ and 28 respectively. The system exhibits chaotic behavior for these and nearby values. Also, the number of steps is defined below.

$$dt = 0.01 + random(-1,1) + random(10^{-14}, 10^{-4}) \tag{2}$$

Here the $random()$ function takes two real numbers as parameters $random(m, n)$ where m is the lower limit and n is the higher limit.

Next, these values a, b, c, x_0, y_0, z_0 and d_t are the seed values for this study which is the set of values that users need to store for generating encryption sequence K_c instead of storing the entirety of K_c. Let, an image I with dimension h pixels in a row while w pixels in column respectively, then, the number of random numbers to be generated are $h \times w$.

Consider the previous iteration of x, y and z are x_{i-1}, y_{i-1} and z_{i-1} respectively. The updated values for x, y and z are given by:

$$\begin{aligned} x_i &= x_{i-1} + dx_i, \\ y_i &= y_{i-1} + dy_i, \\ z_i &= z_{i-1} + dz_i. \end{aligned} \tag{3}$$

Substituting the values of derivatives with equation (4):

$$\begin{gathered} x_i = x_{i-1} + a(y_{i-1} - x_{i-1})dt, \\ y_i = y_{i-1} + (cx_{i-1} - y_{i-1} - x_{i-1}z_{i-1})dt, \\ z_i = z_{i-1} + (x_{i-1}y_{i-1} - bz_{i-1})dt. \end{gathered} \tag{4}$$

Let seed set, S such that:

$$S_c = \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9\} \tag{5}$$

Here, $s_0 = x_{i-1}$, $s_1 = y_{i-1}$, $s_2 = z_{i-1}$, $s_3 = a$, $s_4 = b$, $s_5 = c$, $s_6 = dt$, $s_7 = x$, $s_8 = y$ and $s_9 = z$.

After that, calculate the random value between 0 to 1 using user key S known as $\boldsymbol{S}$. Therefore, K_c is generated using new $\boldsymbol{S}$ value with the total grayscale for 8-bit, 256.

Finally, to encrypt the image, every pixel of the image is traversed. Let I_{ij} represent the plain image matrix, and the encryption sequence be K_c. Every pixel of I will be XORed with the encryption sequence value. Then, it will produce a new encrypted image matrix I_{en1}.

2.2 Encryption Process with Simulated Kalman Filter (SKF) Algorithm

SKF has been introduced by Ibrahim *et. al* in 2015 [10]. This SKF algorithm is inspired by the estimation capability of Kalman Filter. It has been shown that the SKF algorithm performs significantly better than existing metaheuristic algorithms such as Genetic Algorithm (GA) [11]. Since the introduction of SKF, further study has been conducted to have better understanding on the SKF [12]. Furthermore, SKF has undergone significant changes, and many variants of the SKF algorithm have been suggested. The flowchart of SKF algorithm is summarized in Fig. 3.

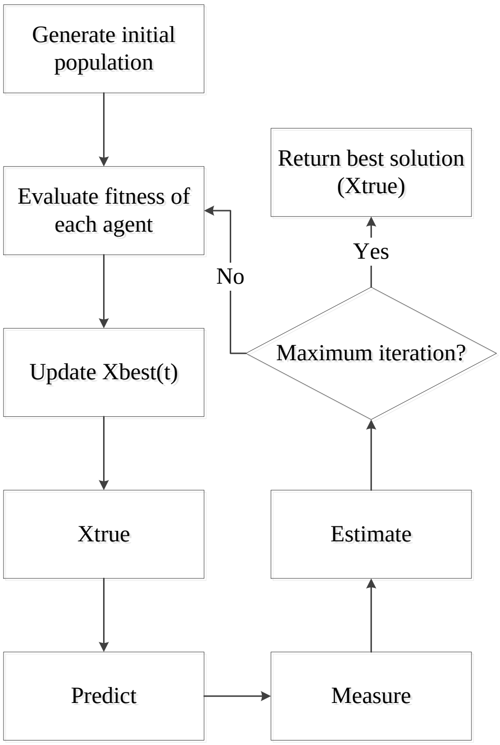

Generate initial population
Evaluate fitness of each agent
Update Xbest(t)
Xtrue
Predict
Measure
Estimate
Maximum iteration?
No
Yes
Return best solution (Xtrue)

Fig. 3. Flowchart of SKF Algorithm (Second Stage)

There is a type of function utilized in the study which is correlation function (6).

$$g(x) = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{\left(N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2\right) \times \left(N\sum_{i=1}^{N} y_i^2 - \left(\sum_{i=1}^{N} y_i\right)^2\right)}} \tag{6}$$

where x and y are gray values of two adjacent pixels in the image. When the entropy coefficients are more generous, the more even is the frequency distribution of the shades in the image and the more the noise. Meanwhile, the algorithm performance is excellent when the correlation coefficient is low, means it is useful in decorrelating and reduces the high correlation in the image.

Initially, the population is set to d, say 20. Then, the random SKF sequence, K_s will be generated 20 in total, $K_{s0}^{0}, K_{s1}^{0}, K_{s2}^{0} \cdots K_{s19}^{0}$ similar to how to generate K_c previously. Thus, each sequence K_{si}^{0} will use a Lorenz seed set. Let the seed set corresponding to the ith sequence denoted as:

$$S_{si}^{0} = \{x_0, y_0, z_0, a + a_{bi}^{0}, b + b_{bi}^{0}, c + c_{bi}^{0}, dt + t_{bi}^{0}\} \tag{7}$$

where for every set S_{si}^{0}, initial Lorenz's state values x_0, y_0 and z_0 remains the same as used by the user in the Lorenz encryption process, only the sampling gap dt and control parameters differ by a value of t_{si}^{0}, a_{si}^{0}, b_{si}^{0} and c_{si}^{0} respectively. The values are generated randomly $10^{-14} \leq t_{si}^0, a_{si}^0, b_{si}^0, c_{si}^0 \leq 10^{-6}$. The superscript 0 represents the generation, in this case, is the initial generation. With the same process as Lorenz chaotic system, from the S_{si}^0, then, K_{si}^0 is spawned. Then, the image I_{en1} is encrypted respected to 20 bat sequences and produce corresponding encrypted images I_{si}^0.

After that, calculate the fitness of each of the images and the sequence which gives the fittest values is chosen among every computed generation, g. Meanwhile, for correlation function, the stopping condition either $CCF \leq 0.0002$ or $g \leq 200$, whichever comes first [7]. And the image with entropy G and correlation CCF, is the final encrypted image, I_{en2}.

2.3 Decryption Process

The decryption process consists of simple steps which are the opposite activity of encryption procedure. First, the user needs to identify the chaotic sequence K_c and SKF sequence K_s that is user key from the previous process. Using the generated keys, the user can decrypt the image, I_{en2}. From there, the final encrypted image will be XORed again with the chaotic sequence K_c and bat sequence K_s, and reproduce the plain or input image, I.

3 Results and Analysis

This subtopic provided with the detailed analysis and outcome of the proposed approach in terms of coefficient correlation, entropy and histogram analysis. It also analyses the sensitivity of the proposed method with refer to NPCR and UACI scores.

3.1 Results

From the proposed methodology, the results below are the outcome of the study. The first stage is based on Lorenz chaotic system which generate the chaotic sequence, K_c. As shown in Fig. 4 is the original Lena image of size 512×512 pixels. Applying the chaotic encryption process, the encrypted image produced denoted as I_{en1}, shown in Fig. 5. The image has correlation coefficient factor (CCF) of 0.00560. From the proposed technique, the control parameters, initial state values and step size in the user key as follows: $a = 15.1111971$, $b = 27.8912200$, $c = 2.6669967$, $x_0 = 21.8787562$, $y_0 = 12.0145000$, $z_0 = 9.1254789$ and $dt = 0.0100356$.

Then, the second part of methodology is the generation of SKF key. The purpose of this encryption sequence to add the second layer of security which minimized the correlation coefficient to the encryption process and increased the image noise. By using Lorenz seed sets are generated previously, random initial population of solutions generates from the SKF algorithm from prediction, measurement, and estimation process. The image in Fig. 6 is the encrypted image after final stage.

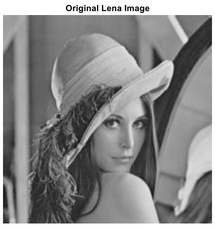


Fig. 4. Original Lena Image

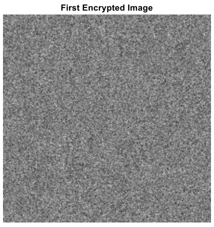


Fig. 5. Encrypted Image after first stage

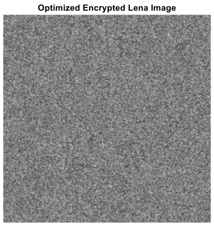


Fig. 6. Encrypted Image after final stage

3.2 Correlation Analysis

Cryptography system security is generally calculated in terms of complexity and uncertainty. As a result, the image is calculated by comparing the similarity of randomly chosen pairs of two adjacent pixels in the original and encrypted images.

Table 1. Analysis of Correlation

Image Name	Plain-image	Ref. [7]	Ref. [8]	Proposed
Lena	0.9718	0.00000682	0.00548	0.00000107

3.3 Entropy Analysis

Entropy is a calculation of the amount of data that needs to be encoded using an acceptable encoding process. The ideal entropy value is 8, suggesting that the method is efficient in extracting randomness from encrypted images and can withstand entropy-based attacks. The analysis of image entropy values is shown in Table 2. The proposed approach outperforms the benchmark by a small margin.

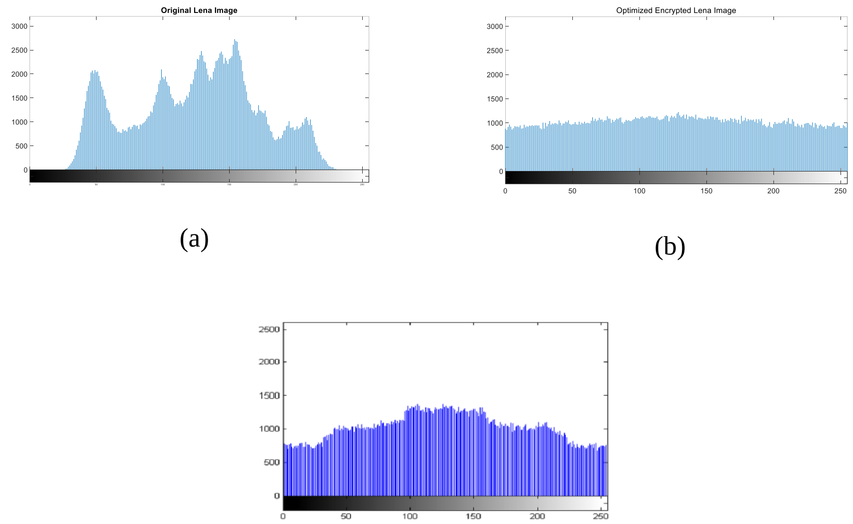
Table 2. Analysis of Entropy

Image Name	Plain-image	Ref. [7]	Ref. [8]	Proposed
Lena	7.57500	7.97200	7.99965	7.99969

3.4 Histogram Analysis

The histogram, or distribution of pixels in an image, is a measure of its randomness material. It shows the overall distribution of different tones in a picture.

Thus, as shown above, an effective encryption effect can be verified by analyzing their histogram plots. From the plots, the pixels distributions of encrypted image illustrated flatter than their plain histogram and Ref. [7].



(a)

(b)

(c)

Fig. 7. (a) Histogram for Plain Image (b) Histogram for Final Encrypted Image (c) Histogram for Ref. [7]

3.5 Differential Analysis

A differential attack can become ineffective if a small change in the plain image causes confusion and diffusion. The cipher picture undergoes a significant shift as well. Parameters like the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) can be used to calculate the effect of a pixel change that is extremely fast in an encrypted picture.

Table 3. NPCR and UACI Scores

Differential Analysis	Ref. [7]	Ref. [8]	Proposed
NPCR (%)	99.23	NA	99.78
UACI (%)	30.15	NA	39.01

NPCR is referred to alteration of plain-image's single pixel while UACI is a value determines the average intensity of differences regarding the plain and encrypted image. From the Table 3, high sensitivity of the proposed method is signified by NPCR and UACI scores with 99.78% and 39.01% respectively compared with Ref. [7].

4 Conclusion

In this study, a new hybrid technique had been proposed to solve image encryption problem such as brute-force attack. The Lorenz chaotic system and an optimization algorithm, Simulated Kalman Filter (SKF) are combined to achieve a great performance with own advantages. SKF algorithm help to increase the noise to the encrypted image and added the key security while chaotic system perfect for secret key generation. From the results and four analyses, the proposed method is outperformed the performance from the benchmarks in literature. To conclude, the proposed hybrid approach is agile and efficient to apply in image encryption problem.

Acknowledgement

The work presented in the paper has been supported by Universiti Malaysia Pahang Post Graduate Research Scheme PGRS2003205.

References

1. Zhao, X., Liu, J., Liu, H., Zhang, F.: Dynamic Analysis of a One-Parameter Chaotic System in Complex Field. IEEE Access. 8, 28774–28781 (2020). https://doi.org/10.1109/access.2020.2968226.
2. Yu, W.B.: Application of chaos in image processing and recognition. 2017 Int. Conf. Comput. Syst. Electron. Control. ICCSEC 2017. 1108–1113 (2018). https://doi.org/10.1109/ICCSEC.2017.8446823.
3. Acharya, B., Panigrahy, S.K., Patra, S.K., Panda, G.: Image Encryption Using Advanced Hill Cipher Algorithm. ACEEE Int. J. Signal Image Process. 1, (2010).
4. Chai, X., Zhang, J., Gan, Z.: Medical image encryption algorithm based on Latin square and memristive chaotic system. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-08168-x.
5. Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y.: An image encryption algorithm based on chaotic system and compressive sensing. Signal Processing. 148, 124–144 (2018). https://doi.org/10.1016/j.sigpro.2018.02.007.

6. Man, Z., Li, J., Di, X., Bai, O.: An Image Segmentation Encryption Algorithm Based on Hybrid Chaotic System. IEEE Access. 7, 103047–103058 (2019). https://doi.org/10.1109/access.2019.2931732.
7. Ahmad, M., Alam, M.Z., Umayya, Z., Khan, S., Ahmad, F.: An image encryption approach using particle swarm optimization and chaotic map. Int. J. Inf. Technol. 10, 247–255 (2018). https://doi.org/10.1007/s41870-018-0099-y.
8. Chikkareddi, V., Ghosh, A., Jagtap, P., Joshi, S., Kanzaria, J.: Hybrid Image Encryption Technique Using Genetic Algorithm and Lorenz Chaotic System. ITM Web Conf. 32, 03009 (2020). https://doi.org/10.1051/itmconf/20203203009.
9. Barrio, R., Dena, A., Tucker, W.: A database of rigorous and high-precision periodic orbits of the Lorenz model. Comput. Phys. Commun. 194, 76–83 (2015). https://doi.org/10.1016/j.cpc.2015.04.007.
10. Ibrahim, Z., Aziz, N.H.A., Aziz, N.A.A., Razali, S., Shapiai, M.I., Nawawi, S.W., Mohamad, M.S.: A Kalman filter approach for solving unimodal optimization problems. ICIC Express Lett. 9, 3415–3422 (2015).
11. Ibrahim, Z., Aziz, N.H.A., Aziz, N.A.A., Razali, S., Mohamad, M.S.: Simulated Kalman Filter: A Novel Estimation-Based Metaheuristic Optimization Algorithm. Adv. Sci. Lett. 22, 2941–2946 (2016). https://doi.org/10.1166/asl.2016.7083.
12. Hidayati, N., Aziz, A., Ibrahim, Z., Razali, S., Bakare, T.A., Aziz, A.A.: How Important the Error Covariance in Simulated Kalman Filter? (2016).