CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.2 / **No.**1 / 2020 / **pp.**17-22

Chaos Theory and its Application: An Essential Framework for Image Encryption

Arshad[*,1], **Shahtaj Shaukat**[‡,2], **Arshid Ali**[†,3], **Amna Eleyan**[§,4], **Syed Aziz Shah**[§,5] **and Jawad Ahmad**[**,6]
[*]Institute for Energy and Environment, University of Strathclyde, Glasgow, United Kingdom, [‡]HITEC University, Taxila, Pakistan, [†]University of Engineering and Technology, Peshawar, Pakistan, [§]Manchester Metropolitan University, Manchester, United Kingdom, [**]School of Computing, Edinburgh Napier University, United Kingdom

ABSTRACT With the advancement in digital technologies and the demand for secure communication, there is an increased interest in the design and implementation of reliable image encryption schemes. This paper presents a thorough review of chaos theory and its application in image encryption schemes. Due to ergodicity and initial key sensitivity, chaos-based image encryption schemes have several advantages over traditional encryption schemes. The paper discusses the major applications of chaos theory, particularly in image encryption area. The use of different chaotic maps such as one and multi-dimensional chaos, hyper and composite chaos in image encryption have been presented. The paper also discusses current trends and future research directions in the field of chaotic image encryption. This work provides a foundation for future research work along with providing basic understanding to new researchers. Several recommendations have been suggested that can improve a chaos-based cryptosystem.

KEYWORDS
Chaos theory
Image encryption
Chaos maps
Logistic map
Composite chaos
Hyper-chaos

INTRODUCTION

In the last few decades, an increasing amount of information needs to be transmitted through the Internet. This information includes text, audio, video, image, and other multimedia data. Digital imaging applications are increasing day by day and there are growing concerns about security, privacy, storage, and confidentiality Chand *et al.* (2015). As the data can be transfer through some medium or channel it may be open-loop network or closed-loop network, public or private network, the only concern is how much the data is secure and how much it is prevented from cyber-attacks. Additionally, data compression is mostly performed to minimize bandwidth usage and storage such as in wireless communication. Furthermore, encryption is also needed to protect the privacy of users Fridrich (1998). The encryption algorithm is used to mask image data streams and provide this security to end-users. These algorithms are based on number-theory and include Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) etc. However, due to the intrinsic features of images such as high redundancy and bulk data capacity, these algorithms are not suited for image encryption. Commonly used image encryption algorithms can be broadly classified into two categories: chaos-based, and non-chaos based Al-Maadeed *et al.* (2012). It can also be further classified into full and partial image encryption based on the amount of image data being encrypted.

The basic building block for any image is the pixel Ahmad and Hwang (2016); Hamid *et al.* (2020). For successful encryption, the information present in each pixel needs to be hidden. The position value of each pixel can also be utilized for encryption. The encryption technique utilized should be strong enough that the encrypted image under testing and decryption at the receiving end.

This paper focuses on the application of famous chaos theory in image encryption. Chaos theory has been used in many applications since 1970. The advantageous prop-

Manuscript received: 12 April 2020,
Revised: 24 April 2020,
Accepted: 29 April 2020.

[1] arshad@strath.ac.uk
[2] shahtajshaukat@gmail.com
[3] arshidali3196@gmail.com
[4] A.Eleyan@mmu.ac.uk
[5] A.Shah@mmu.ac.uk
[6] jawad.saj@gmail.com (**Corresponding Author**)

erties of chaos theory include ergodicity, randomness and sensitivity to initial conditions Yildiz *et al.* (2019); Aziz Shah *et al.* (2020). The paper is organized as follows. Section 2 presents the basic of chaos theory, its application and importance to image encryption. The section provides details about the general image encryption algorithm while section 4 includes detail discussions and literature of chaos-based image encryption. Lastly, future research directions and recommendations are presented in section 5 followed by the conclusion.

CHAOS THEORY

Chaos theory was first discovered by an MIT mathematician and meteorologist Edward Lorenz during the weather prediction experiment in the early 60s. This theory is about to explore the hidden pattern in apparently random data. It provides a convenient way to solve the non-linear problems of natural and artificial systems with their unpredictable behaviours such as road traffic, stock markets, Earthquake, rhythms of a healthy heart, coding sequences of DNA, weather and climatic conditions Anter and Ali (2020). The systems which are highly sensitive to initial conditions can be studied under the umbrella of chaos theory which intentionally referred to a butterfly effect. Butterfly effect usually explained by the idea that a butterfly flaps its wings in Brazil and causes a hurricane in Texas. It means tiny changes in big systems can have complex results. The system, in this case, could be anything from weather patterns to asteroids movement or interaction of a people, with tiny changes the whole system got affected. Scientifically it would be termed as sensitive dependence on initial conditions Dooley (2009).

Various initial conditions are made because of some numerical errors in computations. These errors provide widely diverging results for some dynamic systems. This makes it almost impossible to predict the behaviour of long-term rendering. This happens even when the behaviour of the system is determined by initial conditions of the very same system and no random elements are involved in the process. Dynamic systems with such conditions are known as deterministic. The dynamic system which is not able enough to make them predictable such deterministic behaviour is labelled as deterministic Chaos Šarlošia *et al.* (2014). Thus, an attempt was made by Edward Lorenz in order to describe the main concept of Chaos theory in a single definition. According to him "Present can determine the future, but the approximate present cannot determine approximate future". This predicting randomness issue is kind of a huge problem.

Bifurcation

Bifurcation is one of the main concepts to understand chaos theory. In the non-linear dynamic system, the bifurcation process is observed by an American mathematical physicist Mitchell Feigenbaum in 1975. He described the disorganized behaviour of the system with a simple mathematical model. A model behaviour derives from stability to periodicity and then periodicity to randomness in certain conditions. A system bifurcates and changes its state by applying small perturbation in its guiding rules Thietart and Forgues (1995).

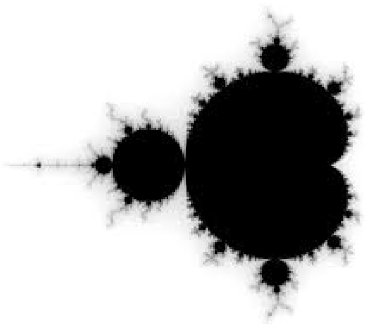

Figure 1 Mandelbrot set Schuster and Just (2006).

Fractals

Fractals are the geometry of chaos or the graphical representations of chaotic function which is related to the study of mathematical science. Never-ending patterns on any scale can be termed as fractals. They are unlike all the usual things in geometry. The things that are initially seemed unrelated but had a very close relationship with each other. If f is the domain of some function f, then the sequence below is the orbit of x for f as:

$$x,\ f\left(x\right), f\left(f\left(x\right)\right)... \tag{1}$$

Mandelbrot and Julia sets are one of the most well-known fractals which can be categorized according to their characteristics, geometry and turbulence.The most eminent Mandelbrot set can be defined as the set of c numbers:

$$\lim_{n\to\infty} |Z_n| \neq \infty \tag{2}$$

Where n is the number of iterations. Point c is related to Mandelbrot set if and only if the limits haven't been determined Šarlošia *et al.* (2014). The Mandelbrot set is shown in Fig.1. Geometric trajectories of the Chaos structure are related to Fractal dimensions. In general:

$$Dimension = \lim_{quantity\to 0} \frac{ln\left(quantity\right)}{ln\left(magnitude\right)} \tag{3}$$

Lorenz Attractor

The data varies over time and it is almost impossible to know all the infinite numbers of data. To understand these theories behind this data approximation is needed. In 1963 Edward Lorenz simplified the atmosphere model and reduced to only three parameters x, y and z. The evolution of the atmosphere was reduced to a simple differential equation:

$$\frac{dx}{dt} = \alpha\left(y - x\right) \tag{4}$$

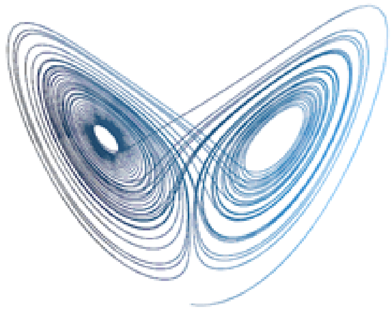

Figure 2 Lorenz attractor Schuster and Just (2006).

$$\frac{dy}{dt} = x(\beta - z) \tag{5}$$

$$\frac{dz}{dt} = xy - \gamma z \tag{6}$$

Where: α is a Prandtl number β is proportional to Reyleigh number γ is a geometric factor

Each point x, y and z represent the state of the atmosphere and progression pursue a vector field Stöckmann (2000). The forecaster just needs to solve the differential equation. This is what Lorenz saw when studied his model. Consider two trajectories of the Lorenz system, with distinct initial conditions. Both trajectories are indeed very different and quite unpredictable but they acquired the same butterfly-shaped object. This accumulation is independent of the initial positions as shown in Fig. 2. One can see from the Fig. 2 that output of this map does not reach to a steady state and hence Lorenz equations are a good example of deterministic chaos. Two different conditions will have different output and will diverge from each other.

In 2001 mathematician Tuckar showed that the paper strip model accurately describes the movement of the Lorenz attractor. For each trajectory in the Lorenz attractor, there is a trajectory in the paper model that behaves exactly in the same way.

Even outside of modelling chaos theory proves exceptionally useful in other fields, such as encryption, global optimization and cloud computing. These are the fields in which chaos theory has been successfully applied, that too with expected results. There are many other fields, in which research is still going on about application of chaos theory. Deterministic systems are the main subject of chaos theory. Chaos theory holds a great concern about these deterministic systems. Especially those systems, whose behaviour can be predicted that is within the scope of principle and related concepts. In the beginning, such chaotic systems tend to be predictable, later on, they turn out to be random. It means chaotic systems are predictable until a specific amount of time from their generation. In a chaotic system, uncertainty in the forecast keeps increasing exponentially. The increment level keeps rising as the time flows on. The more time is passed the more uncertainty should be expected. Thus, according to the mathematical perspective, if the forecast time is doubled the uncertainty will increase more than square value of its current level.

IMAGE ENCRYPTION

The intrinsic feature of the image such as low-cost and high reliability and access at any time, the application of communication system has enhanced that has driven rapid rise it's applications in today's digital world. These days, digital media play an important role when compared to the classical textual mediums as it requires extensive protection to secure the user's privacy. Hence, the safety, security and privacy-preservation of images have attracted several researchers across the globe Masood *et al.* (2020b,a); Shah *et al.* (2019); Ahmad *et al.* (2019). This security can be obtained using digital encryption methods. The digital image encryption refers to the conversion of an image into unreadable human form so that the intruder may not be able to extract any meaningful information. Several services need robust security when storing, transmitting, receiving and sharing digital images Aziz Shah *et al.* (2020). In order to prevent digital image from the use of an unauthorized person, these encryption methods come into play. The digital images are shared over different sort of mediums where a huge portion of this digital data is confidential. The digital encryption is the preferred method to protect data transmission Ahmad and Hwang (2016).

There are different kind of image encryption schemes to encrypt and decrypt the digital image Masood *et al.* (2020a); Ahmad *et al.* (2019). Generally, the vast majority of existing traditional encryption scheme uses text data. These classical or traditional encryption methods can encrypt digital images without any complex mathematics. However, this technique can easily be decrypted by the expert intruder. Initially, the digital image contains specific features including high correlation and huge redundancy. Secondly, these images are typically higher in pixel size making traditional encryption scheme more complex to implement and extremely slow to be encrypted. These plain and simple schemes are feasible for text, however not suitable encrypting multimedia data. These techniques include triple data encryption standard (T-DES) that can provide high security but may not be applicable for multimedia data. For multimedia data, some of the most widely used techniques are Data Encryption Standard (DES), Advanced Encryption Standard (AES).

CHAOS THEORY AND IMAGE ENCRYPTION

Various techniques are used for image encryption/decryption having their advantage and disadvantages. However, one of the most used encryption algorithms in recent time is the chaotic algorithm. There has been an increased interest in chaotic cryptography in the last few years due to the rapid growth and development of chaos theory. Many image encryption schemes have been proposed in literature based on chaos theory Ahmad and Hwang (2016); Patel *et al.* (2020); Ahmad and Hwang

(2015). The increased use of chaos in image encryption is motivated by chaotic properties such as complex dynamics, deterministic behaviours, ergodicity, non-periodicity, pseudo randomness, boundedness and high sensitivity to initial conditions and control parameters.

Compared to conventional encryption techniques, chaos theory is based on the generation of encryption sequence rather than an algorithm and generate a highly random sequence based on the proper selection of a chaotic system. This makes chaotic image encryption much more secure and efficient than conventional encryption schemes Cai (2019). Chaos-based image encryption algorithms can be broadly classified into four main categories: (1) low-dimensional (2) multi-dimensional (3) hyper-chaotic and (4) composite chaotic algorithms. The low-dimensional chaotic algorithms are simple and easy to implement. Typical examples of low-dimensional chaotic encryption algorithms are tent mapping logistic mapping and Chebyshev mapping Li *et al.* (2017); Huang and Yang (2016). However, the disadvantage of low-dimensional chaotic schemes is that these are vulnerable to decoding attacks such as spectrum analysis and phase space reconstruction due to small keyspace and few control parameters.

To overcome this limitation of low-dimensional schemes, researchers have proposed high-dimensional systems having complex dynamical features such as Chen system, Lorenz system and Bao system Lee and Singh (2011); Yassen (2003); Khellat (2015). Increasing the dimension of chaos systems can effectively negate decryption attacks such as phase space reconstruction, however, these algorithms are prone to plaintext attacks. The attacker can decode the control parameters using a few plaintext pairs. To overcome this limitation of multi-dimensional chaos, researchers have integrated chaos theory with other disciplines of image encryption. One such example presented in Chai *et al.* (2017) that propose the use of an encryption algorithm based on DNA coding. These integrated encryption schemes enhance the security of chaos theory and chaotic image encryption. The efficient, secure and robust image encryption, chaotic schemes have been proposed by coupling low and high-dimensional chaos or integrating low-dimensional with hyper-dimensional chaos. The advantage of these schemes is that these can complement each other by protecting chaotic orbit information, support real-time communication and reduce computational complexity Zhu *et al.* (2016).

Seyedzadeh et al. Seyedzadeh and Mirzakuchaki (2012) proposed an algorithm which combines three different chaotic maps (Arnold, Logistic and Kent) for achieving better encryption effect at the expense of a small keyspace. A composite encryption algorithm of low and multi-dimensional chaos has been proposed in Li *et al.* (2019) having the advantage of good random sequence at the expense of weak differential resistance. Based on the above literature, it is evident that for improved encryption performance, a combination of hyper and multi-dimensional chaotic systems need to be designed along with a rational plaintext association strategy. Liu et al. Liu *et al.* (2020) proposed an image encryption scheme based on hyper-chaos integrated with public-key cryptography. By using the four-wing and Chen 4D hyper-chaotic system, two hyper-chaotic random phase masks are constructed. Using the generated hyper-chaotic phase masks and double random phase encoding, the original image is encrypted in the Fresnel domain. The asymmetric encryption of images, a public-key cryptosystem is utilised to allocate and manage the system parameters and initial values. The obtained result shows that the proposed hyper-chaos algorithm has high sensitivity, uniform statistical distribution and the ability to resist noise attacks with low sensitivity coefficient.

A novel colour image encryption schemes have been proposed in Hasanzadeh and Yaghoobi (2019) based on substitution box, fractals and hyper-chaotic dynamics. Julia fractal set is used to generate fractal images in the first phase followed by constructing a substitution box with the help of Hilbert fractals to replace original image pixels with values from the substitution box. For reducing the correlation of the pixel, Logistic map is used to scramble the location of the pixel. The pixel values of fractal images and index production are changed using Chen hyper-chaotic system. In the last step, each pixel of original image layers along with corresponding pixels in the selected fractal images and encrypted pixels values are encrypted with the help of XOR operation. The proposed algorithm showed larger secure keyspace, good encryption effects along with increased sensitivity to plaintext images.

CURRENT RESEARCH TRENDS AND FUTURE RECOMMENDATIONS

From literature, it is evident that chaos theory has a number of applications in the area of cybersecurity. Due to complex dynamics, and pseudorandomness, chaotic maps can be employed in multimedia encryption including audio, video and image. Traditional schemes such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are not well suited for multimedia applications. Due to real-time requirements, novel and light-weight chaos-based encryption algorithms are required. However, chaos-based encryption has several issues which should be kept in mind when designing or proposing a multimedia encryption scheme. For example, some maps have several issues and can lead to an insecure encryption algorithm. Traditional Logistic map has very low keyspace and mathematically, it is written as:

$$x_{n+1} = rx_n(1 - x_n) \quad (7)$$

where, $x_n \in [0,1]$ and $r \in [0,4]$ are known as initial conditions. However, the Logistic map provides a random output when the value of $r \in [3.5699, 4]$. As a result, the encryption scheme based mainly on traditional Logistic map is vulnerable to brute force attack. There are several issues with chaos-based encryption that have been highlighted below. Moreover, we have recommended some suggestions for chaos-based encryption schemes.

Recommendation 1: In future, cryptographers must design such schemes that have sufficient higher keyspace. Traditional one-dimensional maps are vulnerable to attacks if it is not used properly. A hybrid, chaos map can solve such issues.

Recommendation 2: Despite, a high number of schemes are proposed, many of them are either practically not feasible. Due to computational complexity and extensive hardware requirements, many schemes are impractical. Researchers should also discuss and report computational complexity and must report its practical usability.

Recommendation 3: Some researcher does not define the finite precision and floating points which leads to inconsistency. Real number representation must be well defined when proposing a scheme.

Recommendation 4: For some chaos-based encryption schemes, reproducibility of results are not possible due to different mathematical representation of formulas. For example, the Logistic map can also be written as:

$$x_{n+1} = (rx_n - x_n^2). \tag{8}$$

Mathematically, Eq. 1 and Eq. 2 are similar but when using them with different precision and computing representation can lead to unexpected error and incorrect decryption.

Recommendation 5: Many schemes are only compared with other chaos-based encryption schemes. It is highly recommended to compare a proposed scheme with other benchmark encryption schemes. For example, one can compare the proposed scheme with AES etc. However, some authors only compare one aspect and do not discuss other aspects. For example, authors report high keyspace than AES and surprisingly, does not discuss it's complexity.

Recommendation 6: When designing the chaos-based encryption scheme, cryptanalysis driven design approach should not be the only focus As in this approach, the algorithm is tested mainly on statistical analysis. Security results based on statistical analysis could lead to incorrect interpretations. It is highly recommended that some provable secure driven design approach should be proposed. For example, some schemes have good statistical results but fail when ciphertext and plaintext attacks are conducted.

CONCLUSION

In this paper, general chaos theory and its application in real-world has been highlighted. In order to understand chaos theory, one of the important concept 'bifurcation' is reported along with detail discussion. Fractals and Lorenz attractors show that chaos theory can be applied in random number generation and cryptography. A number of image encryption schemes based on the one-dimensional and multi-dimensional scheme are available in the literature. Based on the nature of chaos map, we have highlighted the advantages and disadvantages of the chaos-based encryption scheme. Additionally, we have reported several issues which should be kept in mind when designing an image/multimedia encryption scheme. Several recommendations have been proposed for cryptographers which can help them during the designing phase of an encryption algorithm. For example, keyspace, practical suitability, proper mathematical representation, and comparison with other benchmarks should be part of the research when proposing a chaos-based scheme. In future, we will report a detailed literature review with a novel image encryption using chaos maps. The proposed scheme will be highly secure and will be mainly based on the proposed recommendations.Based on the proposed recommendations made in this paper, a highly secure, lightweight and real-time feasible encryption and decryption algorithm will be proposed.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Ahmad, J. and S. O. Hwang, 2015 Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dynamics **82**: 1839–1850.

Ahmad, J. and S. O. Hwang, 2016 A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications **75**: 13951–13976.

Ahmad, J., A. Tahir, J. S. Khan, M. A. Khan, F. A. Khan, *et al.*, 2019 A partial ligt-weight image encryption scheme. In *2019 UK/China Emerging Technologies (UCET)*, pp. 1–3, IEEE.

Al-Maadeed, S., A. Al-Ali, and T. Abdalla, 2012 A new chaos-based image-encryption and compression algorithm. Journal of Electrical and computer Engineering **2012**.

Anter, A. M. and M. Ali, 2020 Feature selection strategy based on hybrid crow search optimization algorithm integrated with chaos theory and fuzzy c-means algorithm for medical diagnosis problems. Soft Computing **24**: 1565–1584.

Aziz Shah, S., J. Ahmad, A. Tahir, F. Ahmed, G. Russel, *et al.*, 2020 Privacy-preserving non-wearable occupancy monitoring system exploiting wi-fi imaging for next-generation body centric communication. Micromachines **11**: 379.

Cai, Q., 2019 A secure image encryption algorithm based on composite chaos theory. Traitement du Signal **36**: 31–36.

Chai, X., Z. Gan, Y. Lu, Y. Chen, and D. Han, 2017 A novel image encryption algorithm based on the chaotic system and dna computing. International Journal of Modern Physics C **28**: 1750069.

Chand, S., R. Aggarwal, and E. Dubey, 2015 A review of image encryption using chaos based techniques. International Journal of Science and Research **7**: 1871–1875.

Dooley, K. J., 2009 The butterfly effect of the" butterfly effect". Nonlinear dynamics, psychology, and life sciences **13**: 279.

Fridrich, J., 1998 Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos **8**: 1259–1284.

Hamid, H., F. Ahmed, and J. Ahmad, 2020 Robust image hashing scheme using laplacian pyramids. Computers & Electrical Engineering **84**: 106648.

Hasanzadeh, E. and M. Yaghoobi, 2019 A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys. Multimedia Tools and Applications pp. 1–19.

Huang, H. and S. Yang, 2016 Colour image encryption based on logistic mapping and double random-phase encoding. IET Image Processing **11**: 211–216.

Khellat, F., 2015 Delayed feedback control of bao chaotic system based on hopf bifurcation analysis. Journal of Engineering Science and Technology Review **8**: 7–11.

Lee, K. W. and S. N. Singh, 2011 Non-certainty-equivalent adaptive control of chaos in lorenz system. International Journal of Modelling, Identification and Control **13**: 310–318.

Li, C., G. Luo, and C. Li, 2019 An image encryption scheme based on the three-dimensional chaotic logistic map. IJ Network Security **21**: 22–29.

Li, C., G. Luo, K. Qin, and C. Li, 2017 An image encryption scheme based on chaotic tent map. Nonlinear Dynamics **87**: 127–133.

Liu, Y., Z. Jiang, X. Xu, F. Zhang, and J. Xu, 2020 Optical image encryption algorithm based on hyper-chaos and public-key cryptography. Optics & Laser Technology **127**: 106171.

Masood, F., J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, 2020a A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map. Entropy **22**: 274.

Masood, F., J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, 2020b A novel secure occupancy monitoring scheme based on multi-chaos mapping. Symmetry **12**: 350.

Patel, S., R. K. Muthu, *et al.*, 2020 Image encryption decryption using chaotic logistic mapping and dna encoding. arXiv preprint arXiv:2003.06616 .

Šarlošia, J., J. Bockob, and R. Suroveca, 2014 Deterministic chaos. Procedia Engineering **96**: 458–466.

Schuster, H. G. and W. Just, 2006 *Deterministic chaos: an introduction*. John Wiley & Sons.

Seyedzadeh, S. M. and S. Mirzakuchaki, 2012 A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal processing **92**: 1202–1215.

Shah, S. I., S. Y. Shah, and S. A. Shah, 2019 Intrusion detection through leaky wave cable in conjunction with channel state information. In *2019 UK/China Emerging Technologies (UCET)*, pp. 1–4, IEEE.

Stöckmann, H.-J., 2000 Quantum chaos: an introduction.

Thietart, R.-A. and B. Forgues, 1995 Chaos theory and organization. Organization science **6**: 19–31.

Yassen, M., 2003 Chaos control of chen chaotic dynamical system. Chaos, Solitons & Fractals **15**: 271–283.

Yildiz, M. Z., O. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, 2019 A novel encryption method for dorsal hand vein images on a microcomputer. IEEE Access **7**: 60850–60867.

Zhu, H., X. Zhang, H. Yu, C. Zhao, and Z. Zhu, 2016 A novel image encryption scheme using the composite discrete chaotic system. Entropy **18**: 276.

How to cite this article: Arshad, Shaukat S., Ali, A., Eleyan, A., Shah, S. A., and Ahmad, J. Chaos Theory and its Application: An Essential Framework for Image Encryption. Chaos Theory and Applications, 2(1), 17-22, 2020.