International Journal of Innovative Research & Growth
A Peer Reviewed Journal
ISSN: 2455-1848
Journal homepage: http://www.ijirg.com/ijirg/
Volume: 11 Issue: 1, January 2022

Encryption algorithms using chebyshev chaotic map: a survey

Saumya Neekhara[1], Sandeep K. Tiwari[2*], Anand Singh Bisen[3]
[1]Research Scholar, Vikrant Institute of Technology and Management, Gwalior, M. P., India
[2,3]Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Gwalior, M. P., India
E-mail: saumyanekhara0661997@gmail.com , sandeep72128@gmail.com, anandsingh@vitm.edu.in
* Corresponding Author

Article Info
Received 20 November 2021
Received in revised form 19 December 2021
Accepted for publication 19 January 2022
DOI: 10.26671/IJIRG.2022.1.11.104
Citation:
Neekhara, S., Tiwari, S. K., Bisen, A. S. (2022). Encryption algorithms using chebyshev chaotic map: a survey. *Int J Innovat Res Growth*, 11, 17-19.

Abstract
Nowadays the use of Internet is increasing exponentially. Most of the people use Internet for running social media apps and websites. People use these social media apps to share images and videos. These images and videos contain personal information of the user and needs to be protected. Several encryption algorithms have been developed to maintain the privacy and security of the user. This work describes the various encryption algorithms based on Chebyshev chaotic map. By using this work, researchers can get a detailed overview of Chebyshev chaotic map in different encryption algorithms.
Keywords: - Encryption, Decryption, Chebyshev chaotic map, Chaotic map, Image Encryption.

1. Introduction

In current scenario, privacy and security of user's data over the internet is become the primary concern before researchers. For achieving this, most of the researchers are working in this field. Many encryption algorithms have been developed for securing user's data over the internet. Some algorithms are based on symmetric key and others are based on asymmetric key. Chaotic map is one of the choices in encryption algorithm in terms of randomness. Many chaotic maps such as Chebyshev chaotic map, logistic chaotic map, sine map, tent map, etc, have been developed to achieve randomness. Each chaotic map has its own advantages and disadvantages. This work presents a survey of Chebyshev chaotic map based encryption algorithms.
The motivation behind this work is to check the effectiveness of Chebyshev chaotic map by using different techniques and application. This will help various researchers to use this chaotic map in latest research.
The rest of the paper is summarized as follows: Section 2 gives detailed overview of various encryption algorithms based on Chebyshev chaotic map along with deep analysis. Section 3 concludes the overall work.

2. Literature Review

This section describes the detailed description of various encryption algorithms based on Chebyshev chaotic map. This paper [1] proposed a Chebyshev maps-based public-key encryption algorithm that is secure, practical, and can be used for both encryption and digital signature. The algorithm's software implementation and properties are explored in depth.
Chebyshev polynomials have recently been suggested as a tool for building public-key schemes. They do, in particular, have some interesting chaotic properties that tend to be suitable for use in cryptography. They also satisfy a semi-group property, allowing for the introduction of a trapdoor mechanism. This work [2] analyzes a public-key cryptosystem based on such polynomials that can provide both encryption and digital signature in this paper. The cryptosystem is very effective and operates for real numbers.
The methods for constructing spread-spectrum sequences with a Mach-Zehnder interferometer are explored, as well as the theory and scheme of a previously described Chebyshev chaotic sequence generator [3]. A new scheme based on the properties of the cosine function is proposed to address the constraint faced by the size of optical components. A wavelength adaptive generator can be realized by using voltage to change the refractive index of the arms of a Mach-Zehnder interferometer, allowing various Chebyshev optical chaotic sequences of different input wavelengths to be collected.
This paper [4] presents a chaotic image encryption algorithm that uses a nonlinear Chebyshev function to generate the key stream. With the generated secret keys relying on each other, a novel method of constructing pseudorandom chaotic sequences is used. Then, to minimize the strong similarity between adjacent pixels in the original plain image, we make several permutations of pixels. Furthermore, in the diffusion method, a two-dimensional Chebyshev feature is assumed to

prevent known-plaintext and chosen-plaintext attacks, i.e., even if the initial plain image was modified by one bit, the encrypted image will be drastically different.

A new multi-chaos based image encryption algorithm is introduced in this article [5]. The encryption algorithm employs four chaotic mappings. The state of Chebyshev mapping decides the renew feature of CML mapping. CML and Chebyshev iteration are used to achieve pixel value encryption and pixel location permutation. The encryption algorithm has higher security, according to research and experimental findings.

Recent studies of image encryption algorithms have been increasingly based on chaos, but chaotic cryptosystems still have flaws that pose a security risk. In this article [6], we conduct cryptanalysis on a Chebyshev chaotic map-based image encryption and discover the following: (1) the scheme can be broken by a chosen-plaintext attack. (2) For the encryption scheme, there are identical keys and weak keys. (3) The scheme is immune to changes in the plain image. We have carried out the chosen-plaintext attack successfully. A remedial approach is recommended to overcome the disadvantages.

The Chebyshev polynomial based on permutation and substitution, as well as the Duffing map based on substitution, is used in this work [7] to show a novel image encryption algorithm. Key space analysis, visual checking, histogram analysis, information entropy estimation, correlation coefficient analysis, differential analysis, key sensitivity evaluation, and speed test were all used to do a detailed security analysis on the designed scheme. Based on strong observational findings and theoretical reasons, the study indicates that the proposed image encryption algorithm has advantages of more than key space and a desirable degree of security.

This paper [8] suggested a new image encryption algorithm based on two distinct pseudorandom bit generators: Chebyshev map and rotation equation. The first is used for permutation, and the second is used for substitution. Visual testing, key space analysis, histogram analysis, information entropy estimation, correlation coefficient analysis, differential analysis, key sensitivity test, and numerical and complexity analysis have all been used to provide a comprehensive security analysis on the novel image encryption algorithm. The novel image encryption scheme shows an excellent degree of protection based on theoretical and analytical evidence.

This work [9] introduced a class of public-key cryptosystems called multiplicative coupled cryptosystem, or MCC for short, as well as explores its security within three different models. Furthermore, for these three security models, this work addresses a disorderly instance of MCC based on the first and second forms of Chebyshev polynomials over real numbers. The Chebyshev polynomials of the first and second forms over a finite field are used to prevent round-off errors in floating point arithmetic and to increase the security of the chaotic instance discussed. The suggested MCCs' performance is also taken into consideration.

It's become standard practice in cryptography to use nonlinear (chaotic) transformations to generate chaos during the encryption process. In this article [10], a pair of capable cryptosystem techniques based on substitution and permutation on a one-dimensional chaotic map was proposed (Improved Chebyshev map). The construction of an S-box using a one-dimensional chaotic structure is first introduced as an efficient and simple process. The main benefit of the proposed scheme is that it produces solid S-boxes dependent on the keys used by the chaotic map. Then, using the substitution box and the chaotic map (substitution and permutation system), an efficient encryption scheme is presented.

Based on one-dimensional chaotic Chebyshev mappings, this study creates a novel randomized chaotic image encryption algorithm. The permutation is applied to image pixels using a novel chaotic breadth-first search algorithm, which is described first. This work [11] also uses a novel approach to create the diffusion matrix using a chaotic sequence. As opposed to hyper-chaotic encryption schemes, using a one-dimensional chaotic mapping in the development of an image encryption algorithm has the advantage of lower computational and space complexities.

The dynamical behavior of a new 2D Chebyshev-Sine map with normal evaluation is studied [12]. A color image encryption algorithm is designed to examine its use in information security. Before each encryption process, a one-time initial state represented as an ordered quaternion is derived from colored non Gaussian noise. By using an exclusive or (XOR) operation with an avalanche effect, the algorithm will achieve the desired effect after two cycles. Since the algorithm's speed is high, it's ideal for image encryption over the cloud, according to simulation results.

For color image encryption, a novel random chaotic asymmetric-key algorithm is proposed in this article[13]. A novel chaotic key establishment algorithm based on Chebyshev polynomials is proposed using the multiplicative coupled Chebyshev-based encryption algorithm. The simple image's rows and columns are uniformly permuted using this main establishment algorithm, which produces three chaotic pseudo-random number sequences. Then, to obscure the value of each pixel, it is XORed with a random value extracted from its new position. Since the entire encryption algorithm is randomized, it can survive targeted plaintext attacks.

3. Conclusion

This work gives a detailed overview of encryption schemes based on Chebyshev chaotic map. With the help of this work, researchers can get a detailed overview of the use of Chebyshev chaotic map in different techniques and applications. Also, this work provides the effectiveness of Chebyshev chaotic map, which will help to the researchers for using Chebyshev chaotic map in latest research.

Conflict of Interest

In this manuscript the authors declare that there is no conflict of interest.

References

i. Kocarev, L., Tasev, Z. (2003). Public-key encryption based on Chebyshev maps. *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03*. 3. IEEE, III–III. doi: 10.1109/ISCAS.2003.1204947.

ii. Bergamo, P., D'Arco, P., Santis, A. D., Kocarev, L. (2005). Security of public-key cryptosystems based on Chebyshev polynomials. In *IEEE Transactions on Circuits and Systems I: Regular Papers*, 52, 1382-1393. doi: 10.1109/TCSI.2005.851701.

iii. Liu, H. S., Xin, X. J., Yin, X.L., Yu, C. X., Zhang, Q. (2009). An optimization scheme for generating of Chebyshev optical chaotic sequence. *Acta Phys Sin.* 58, 2231–2234.

iv. Huang, X. (2012). Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn.* 67, 2411–241. https://doi.org/10.1007/s11071-011-0155-7

v. Lin, N., Guo, X., Xu, P., Wang, Y. (2013). A New Multi-chaos Based Image Encryption Algorithm. In: Du Z. (eds) Intelligence Computation and Evolutionary Computation. Advances in Intelligent Systems and Computing, 180. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31656-2_32

vi. Wang, X., Luan, D., Bao, X. (2014). Cryptanalysis of an image encryption algorithm using Chebyshev generator. *Digital Signal Process*, 25, 244–247.

vii. Stoyanov, B., Kordov, K. (2014). Novel Image encryption scheme based on Chebyshev polynomial and duffing map. *Sci World J.*, 283639, 11. https://doi.org/10.1155/2014/283639

viii. Stoyanov, B., Kordov, K. (2015). Image encryption using Chebyshev map and rotation equation. Entropy. 17,2117–2139. https://doi.org/10.3390/e17042117

ix. Shakiba, A., Hooshmandasl, M. R., Meybodi, M. A. (2016). Cryptanalysis of multiplicative coupled cryptosystems based on the Chebyshev polynomials. Int J Bifurcation Chaos. 26, 1650,112.

x. Attaullah, Javeed, A., Shah, T. (2019). Cryptosystem techniques based on the improved Chebyshev map: an application in image encryption. Multimed Tools Appl., 78, 31467–31484. https://doi.org/10.1007/s11042-019-07981-8

xi. Shakiba, A. (2019). A novel randomized one-dimensional chaotic Chebyshev mapping for chosen plaintext attack secure image encryption with a novel chaotic breadth first traversal. *Multimed Tools Appl.*, 78, 34773–3479. https://doi.org/10.1007/s11042-019-08071-5

xii. Liu, H., Wen, F., Kadir, A. (2019). Construction of a new 2D Chebyshev-Sine map and its application to color image encryption. *Multimed Tools Appl.*, 78, 15997–16010. https://doi.org/10.1007/s11042-018-6996-z

xiii. Shakiba, A. (2021). A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad. Journal of King Saud University-Computer and Information Sciences, 33, 562-571. https://doi.org/10.1016/j.jksuci.2019.03.003