Commentary
Volume 15:8, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

A Inter Diffusion Based Encryption Algorithm on Advanced Connectivity Modification

Forbes Richard*

Department of Information Science, University of Pennsylvania, Philadelphia, PA 19104, USA

Introduction

When keys are transmitted over public channels, they are vulnerable to a variety of security threats. We propose an image encryption algorithm based on complex network scrambling and multi-directional diffusion in this paper. The RSA algorithm is used to encrypt the key associated with plaintext, combining the idea of public key cryptography. The algorithm is divided into three stages: key generation, complex network scrambling, and multi-directional diffusion. To begin with, during the key generation phase, SHA-512 and the original image are used to generate plaintext-related information, which is then transformed into a plaintext-related key via transformation mapping. Second, in the complex network scrambling stage, the chaotic random matrix establishes the node relationships in the complex network, which is then used to construct an image model based on the complex network and then scramble images by combining pixel-level and block-level methods. Finally, in the multi-directional diffusion stage, the multi-directional diffusion method is used to perform forward diffusion, middle spiral diffusion, and backward diffusion on the image in turn to obtain the final ciphertext image.

Description

The experimental results show that our encryption algorithm has a large keyspace, the encrypted image has strong randomness and robustness, and can effectively resist brute force attack, statistical attack, and differential attack [1-3]. A large number of digital images are transmitted on the network in this era of rapid information technology development. Satellite images can reveal a wealth of information, such as the distribution of city buildings and crop growth; medical images can reveal health status, age information, and so on. Images containing sensitive information, such as military secrets, commercial information, and government documents, are also available. Furthermore, when images are transmitted over public networks, security risks such as interception, tampering, and copying may occur. As a result, academics are becoming increasingly concerned about image security.

Image encryption is an effective method of image security. Traditional text encryption schemes include DES, AES, and others. When using these schemes to encrypt images, the image must first be converted into a bit stream, which ignores the high information content, redundancy, and correlation between pixels. As a result, traditional image encryption schemes have drawbacks and are not suitable for image encryption [4,5]. As a result, developing new efficient and secure image encryption algorithms has emerged as a critical research topic in the field of security. Because chaotic systems have properties like initial value and parameter sensitivity, ergodicity, and unpredictability, they are well suited for image encryption. Scholars have proposed numerous image encryption algorithms based on chaos theory. Hu et al., for example, proposed a coupled chaotic system based on unitary transformation that can combine two one-dimensional chaotic systems into a chaotic system with improved performance, on which an image encryption algorithm was designed to encrypt the high and low parts of an image separately.

Conclusion

Complex network theory evolved from graph theory in mathematics, which can represent interactions or relationships within complex systems. Complex networks are made up of nodes and edges. Transportation networks comprised of linked cities and highways, as well as the Internet comprised of computers and networks, are examples of complex networks in everyday life. Complex networks now have numerous applications in social sciences, control engineering, and secure communication. Many existing image encryption algorithms employ symmetric cryptosystems, which use the same key for encryption and decryption. As a result, securing the key during encryption and decryption is difficult. In asymmetric cryptosystems, however, the public key of the receiver is used for encryption, while the private key of the receiver is used for decryption. As a result, asymmetric cryptosystems can address the issue of key security during transmission.

Acknowledgement

None.

Conflict of Interest

Authors declare no conflict of interest.

References

1. Dalleck, Lance C., Erica C. Borresen and Amanda L. Parker. "Development of a metabolic equation for the NuStep recumbent stepper in older adults." *Percept Mot Skills* 112 (2011): 183-192.
2. Fours, Baptiste, Yohann Cartigny and Samuel Petit. "Formation of new polymorphs without any nucleation step. Desolvation of the rimonabant monohydrate: Directional crystallisation concomitant to smooth dehydration." *Faraday Discuss* 179 (2015): 475-488.
3. Bai, Guoying, Dong Gao and Zhang Liu. "Probing the critical nucleus size for ice formation with graphene oxide nanosheets." *Nat* 576 (2019): 437-441.
4. Blum, Lorenz C., and Jean-Louis Reymond. "970 million druglike small molecules for virtual screening in the chemical universe database GDB-13." *J Am Chem Soc* 131 (2009): 8732-8733.
5. Meringer, Markus, and Emma L. Schymanski. "Small molecule identification with MOLGEN and mass spectrometry." *Metabolites* 3 (2013): 440-462.

***Address for Correspondence:** Forbes Richard, Department of Information Science, University of Pennsylvania, Philadelphia, PA 19104, USA, E-mail: ForbesRichard4@gmail.com*

Date of Submission: 07 August, 2022, Manuscript No. jcsb-22-79090; **Editor assigned:** 09 August, 2022, Pre QC No. P-79090; **Reviewed:** 23 August, 2022, QC No. Q-79090; **Revised:** 28 August, 2022, Manuscript No. R-79090; **Published:** 02 September, 2022, DOI: 10.37421/0974-7230.2022.15.430

How to cite this article: Richard, Forbes. "A Inter Diffusion Based Encryption Algorithm on Advanced Connectivity Modification." J Comput Sci Syst Biol 15 (2022):430.