Received: 04 June 2022 | *Revised:* 22 June 2022 | *Accepted:* 24 June 2022
DOI: 10.37917/ijeee.18.2.9 *Vol. 18| Issue 2| December 2022*

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences

Ghofran Khaled Shraida, Hameed Abdulkareem Younis
Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

Correspondence
*Ghofran Khaled Shraida
Department of Computer Science, College of CSIT,
University of Basrah, Basrah, Iraq
Email: itpg.ghofran.khaled@uobasrah.edu.iq

Abstract
Experts and researchers in the field of information security have placed a high value on the security of image data in the last few years. They have presented several image encryption techniques that are more secure. To increase the security level of image encryption algorithms, this article offers an efficient diffusion approach for image encryption methods based on one-dimensional Logistic, three-dimensional Lorenz, DNA encoding and computing, and SHA-256. The encryption test demonstrates that the method has great security and reliability. This article, also, examines the security of encryption methods, such as secret key space analysis, key sensitivity test, histogram analysis, information entropy process, correlation examination, and differential attack. When the image encryption method described in this article is compared to several previous image encryption techniques, the encryption algorithm has higher information entropy and a lower correlation coefficient.

KEYWORDS: Chaos theory, Deoxyribonucleic Acid (DNA), hash function, image encryption, logistic map, Lorenz attractor.

I. INTRODUCTION

Since the Internet's introduction into our lives, information security has become critical. With practically everything are available to anybody on the world with a few mouse clicks, protecting personal information on the Internet is important. One method of safeguarding information is to convert the image into an unintelligible form that seems to be a random noisy image. Image encryption is the name given to this method. For a long time, image encryption has piqued the curiosity of scholars all over the world. Image encryption employs certain conventional encryption methods, such as, DES, AES, and RSA [1], [2]. However, when used to a system that encrypts a huge number of images or video, the conventional encryption technique is less efficient. As a result, the necessity to create unique image encryption techniques arises. In the realm of information encryption, the chaotic system possesses better features. Chaos possesses a number of complicated qualities that aid in the development of more safe and durable encryption schemes. It is sensitive to beginning value circumstances, unpredictable, and has a high bifurcation complexity [3], [4]. Chaotic patterns contain Hénon map, Lorenz map, logistic map, Arnold Cat map, and others [5]. This complexity of chaotic mapping may be seen in the features of some encryption processes that are comparable to ideal ciphers, such as, avalanche, balancing, aliasing, and diffusion [6]. Some encryption methods based on chaos theory are devised and used to image encryption in order to assure the security of image information during transmission and storage.
Furthermore, several of the outstanding characteristics of deoxyribonucleic acid (DNA) computing have lately been discovered, for example: tiny energy loss, huge storage space, and large-scale computational parallelism. As a result, the employment of complementary DNA principles to encrypt information technology has made significant progress. Therefore, the algorithms based on DNA and chaotic system use the advantages of both fields to provide image protection in an effective way. [7]–[10] These research papers proposed merging DNA coding and chaos theory in image encryption schemes. In [11] a unique color image encryption technique using one-time pad was proposed. To improve the robustness of the suggested algorithm, the secret keys and the Hamming distances between the DNA matrices are used to construct the key streams from the 3D Skew Tent Map (3D-STM). In [12] a new encryption and decryption technique for validating image transfer across information correspondence frameworks was presented. Both are indistinguishable using hybrid chaotic confusion processes and the mitochondrial DNA (mtDNA) diffusion technique, which reduce equipment use complexity and enhance framework security. In [13] a novel DNA-based RGB image encryption algorithm using the hash function SHA-256 and the Nonlinear Chaotic Algorithm (NCA) map-based Coupled Map Lattice (CML)