International Journal of Applied Science-Research and Review
ISSN: 2394-9988
Open access
Commentary

Cutting-edge Image Encryption with Hyperchaotic Systems, DNA Computing, and SHA-512 Hash Functions

Cyrus Lange*
Department of Applied Science, University of Debrecen, Hungary

DESCRIPTION

A new hyperchaotic image encryption scheme based on DNA computing and SHA-512 presents a sophisticated approach to enhancing the security of digital images. This method combines advanced cryptographic techniques with the innovative principles of DNA computing and the robustness of the SHA-512 hashing algorithm to create a highly secure encryption system. The complexity and novelty of this scheme offer promising solutions for safeguarding sensitive visual information against unauthorized access and cyber threats. Hyperchaotic systems are characterized by their extreme sensitivity to initial conditions and their ability to generate complex, unpredictable sequences. These properties make hyperchaotic systems particularly suitable for cryptographic applications, as they can produce encryption keys that are highly resistant to decryption attempts. In the context of image encryption, a hyperchaotic system generates a sequence of pseudo-random numbers that are used to encrypt and decrypt image data, ensuring that the encrypted output is substantially different from the original image. The integration of DNA computing principles adds another layer of security and complexity to the encryption scheme. DNA computing leverages the unique properties of biological DNA to perform complex calculations and data processing tasks. In the proposed encryption scheme, DNA-based operations are employed to enhance the encryption process, making it more intricate and less susceptible to conventional attacks. DNA sequences are used to generate encryption keys and manipulate image data, exploiting the parallelism and massive storage capacity inherent in DNA molecules. The SHA-512 algorithm, part of the SHA-2 family of cryptographic hash functions, is used to provide additional security to the encryption scheme. SHA-512 generates a 512-bit hash value from input data, ensuring a high level of data integrity and collision resistance. By incorporating SHA-512 into the encryption process, the scheme benefits from a robust hashing mechanism that further strengthens the security of the encrypted images. The hash values produced by SHA-512 are used to initialize and control the hyperchaotic system, adding an extra layer of unpredictability to the encryption keys. In practice, the encryption scheme operates through several stages. First, the image data is converted into a format suitable for processing by the hyperchaotic system. This involves breaking down the image into smaller blocks and applying pre-processing techniques to prepare the data for encryption. The hyperchaotic system generates a sequence of pseudo-random numbers based on the initial conditions set by the SHA-512 hash values. These numbers are used to scramble the image data, transforming it into an encrypted form that is visually indistinguishable from random noise. The DNA computing component comes into play by using DNA sequences to manipulate the encrypted image data further. Operations such as DNA-based pattern matching and sequencing are employed to enhance the complexity of the encryption process. This additional manipulation ensures that the encryption scheme remains resistant to various cryptographic attacks, including brute force and pattern recognition attempts. To decrypt the image, the process is reversed. The encrypted data is processed using the same hyperchaotic system and DNA-based operations, guided by the SHA-512 hash values. This ensures that the original image can be accurately restored, provided that the correct encryption keys and parameters are used. The robustness of the hyperchaotic system, combined with the complexity introduced by DNA computing and SHA-512, makes it highly challenging for unauthorized users to decrypt the image without proper access to the encryption keys. In summary, the new hyperchaotic image encryption scheme based on DNA computing and SHA-512 offers a cutting-edge solution for securing digital images.

ACKNOWLEDGEMENT

None.

CONFLICT OF INTEREST

The author declares there is no conflict of interest in publishing this article.

Received:	31-July-2024	**Manuscript No:**	IPIAS-24-21463
Editor assigned:	02-August-2024	**PreQC No:**	IPIAS-24-21463 (PQ)
Reviewed:	16-August-2024	**QC No:**	IPIAS-24-21463
Revised:	21-August-2024	**Manuscript No:**	IPIAS-24-21463 (R)
Published:	28-August-2024	**DOI:**	10.36648/2394-9988-11.4.35

Corresponding author Cyrus Lange, Department of Applied Science, University of Debrecen, Hungary, E-mail: CyrusLange536745@yahoo.com

Citation Lange C (2024) Cutting-edge Image Encryption with Hyperchaotic Systems, DNA Computing, and SHA-512 Hash Functions. Int J Appl Sci Res Rev. 11:35.