IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

COLOR IMAGE ENCRYPTION USING DNA WITH QUANTUM WALK ALGORITHM

Apoorva N Mattur
Dept. Of Computer Science and Engineering
PES Institute of Technology and Management
Shimoga, India

Bhairavi N Udupa
Dept. Of Computer Science and Engineering
PES Institute of Technology and Management
Shimoga, India

Chandana T N
Dept. Of Computer Science and Engineering
PES Institute of Technology and Management
Shimoga, India

Divya S
Dept. Of Computer Science and Engineering
PES Institute of Technology and Management
Shimoga, India

Mr. Sandeeep K H
Dept. of Computer Science and Engineering,
PES Institute of Technology and Management
Shimoga, India

Abstract— **As there is a rapid increase in demand for secure image transmission in various fields, image encryption has its own importance in cryptography. DNA computing and quantum walk offer unique advantages for robust encryption. Traditional image encryption algorithms face challenges from quantum computing. The proposed scheme offers a promising approach to color image encryption with enhanced security and potential for quantum-resistant cryptography. Not only it is secure, but this method is also sensitive to small changes in the secret key used to unblock the image. Swapping a single letter in the key would scramble the picture completely. The proposed method makes it safe from unauthorized access.**

Keywords—Encryption, DNA encoding, Quantum walk, SHA-256 Hashing, chaotic system.

I. INTRODUCTION

Cryptography is technique of securing information and communications through use of codes so that only that person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. Cryptography aims to keep data and messages private and inaccessible to possible threats. It frequently works invisibly to encrypt and decrypt the data you send through email, social media, applications, and website interactions.

Deoxyribonucleic acid (DNA) computing is a bioscience-inspired technology that uses DNA as an information carrier for secure communications over networks [8]. The molecular structure of DNA and its complex processes such as hybridization or polymerase chain reaction (PCR) provide tremendous parallelism, energy efficiency, and superior storage capacity. It is one of the most advanced forms of information representation. Therefore, there is a trend in cryptography to develop many new algorithms to secure data [3]. In DNA computational cryptography, information is encrypted in a DNA sequence using molecular computation, whereas existing conventional cryptography uses complex mathematical procedures for encryption. This chapter discusses the DNA computational techniques proposed by different researchers for different encryption goals such as encryption and decryption, authentication, digital signatures, and the challenges of implementing DNA computation in cryptography [4].

Quantum hash function is an important area of interest in the field of quantum cryptography [5]. Quantum hash function based on controlled alternate quantum walk is a mainstream branch of quantum hash functions by virtue of high efficiency and flexibility [5].

II. BACKGROUND

Works on making computer programs called Deep Neural Network (DNN) smarter, especially for diagnosing medical conditions. To do this, powerful cloud servers are used. However, these servers aren't perfect when it comes to keeping things private. Because medical information is sensitive, there's a concern about privacy when using these servers. To solve this, a special way of hiding or "encrypting" the medical images used to train these programs. This new method is better than previous ones and helps train the programs while keeping the private medical information safe. To prove that their method works well, many tests have been ran using medical data available to the public. The results show that their improved encryption method is effective, both in terms of making the programs work better and keeping the private medical data secure.

The "Color Image Encryption Algorithm Based on a Chaotic Model" is like a special recipe that mixes up the colors in the picture in a very complicated and unpredictable way. This method is inspired by chaos theory, a branch of mathematics dealing with complex and unpredictable systems. So, when encryption algorithm is used on a picture, it transforms the colors into a jumbled-up version. To anyone who doesn't have the right "key" (like a secret password), the picture will just look like a confusing mess. But if the key is known, one can unscramble the colors and see the original picture.

The encryption method mainly has SHA-512, which is like a secret formula. It jumbles the picture in a way that seems like a confusing mess to anyone who doesn't know the secret. But if one has the right key (a secret code), he can unscramble the picture and see it normally. So, it's a way of making sure only people with the right code can see the pictures and keep them safe from others. The special code inspired by the way humans DNA, the genetic material in living things, works. This code transforms the message into something that looks like a jumble of letters, but only someone with the right key (like a secret password) can turn it back into the original message. It's like having a secret language that helps keep the information safe from people who don't know the special code.

III. SYSTEM DESIGN

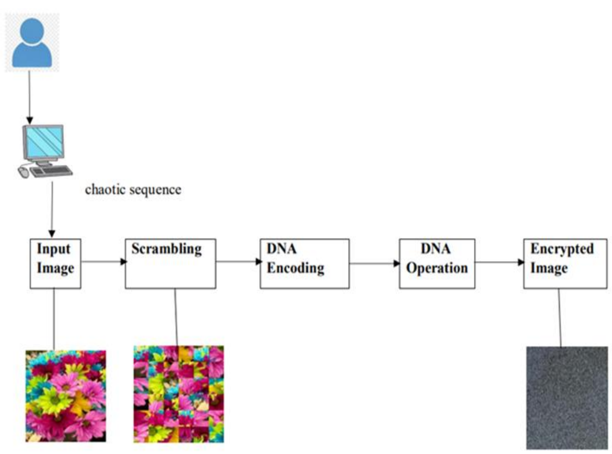

Fig.1. System Architecture

A. Why Quantum Walk?

Quantum walks exploit superposition and entanglement, which are fundamental principles of quantum mechanics. This makes them inherently more difficult to analyse and break compared to classical scrambling algorithms. This property is especially valuable for highly sensitive information. Quantum walks can generate complex and unpredictable sequences, leading to thorough image scrambling and resistance to statistical attacks. This randomness enhances the overall security of the process. Quantum algorithms can have the capabilities of quantum computers to perform scrambling operations much faster than classical algorithms on traditional computers. This speedup could be significant for large images or real-time applications.

IV. METHODOLOGY

- The process begins with a color image, typically in a format like JPEG or PNG. The RGB color channels of the image are extracted and combined into a one-dimensional array of pixel values. A quantum walk algorithm is applied to this array, generating a random sequence of indices. The pixel values are rearranged based on this sequence, scrambling the image's visual content.

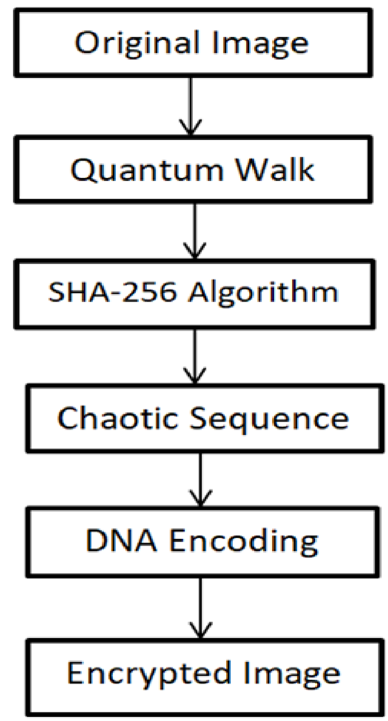

Fig. 2. Flow Chart

- The scrambled image is processed using the SHA-256 hashing algorithm. This generates a unique 256-bit message digest, which serves a dual purpose as acts as a unique identifier for the image, ensuring integrity during transmission and it is used as the initial condition for the chaotic system in the next step.
- The message digest is inputted into a high-dimensional chaotic system. The chaotic system generates a new random sequence, characterized by high sensitivity to initial conditions and unpredictability. This sequence will control the DNA encoding process in subsequent steps.
- The chaotic sequence is used to choose eight different DNA coding rules. The pixel's original value is broken down into eight distinct signals (8-bit binary). These signals are paired up, ready for translation. It pairs each signal duo with a specific DNA base (A, C, G, or T), crafting a unique 4-letter DNA word. The chaotic sequence also determines the number of DNA encryption iterations for the pixel. In each iteration, the DNA sequence undergoes transformations (e.g., XOR operations).
- After the prescribed transformations, the final DNA word is translated back into a new, unrecognizable number (decimal equivalent). This number replaces the pixel's original value, successfully masking its identity within the image. After all pixels have undergone DNA encoding, the process yields a fully encrypted image. The visual content of the encrypted image bears no resemblance to the original image.

V. RESULTS AND DISCUSSION

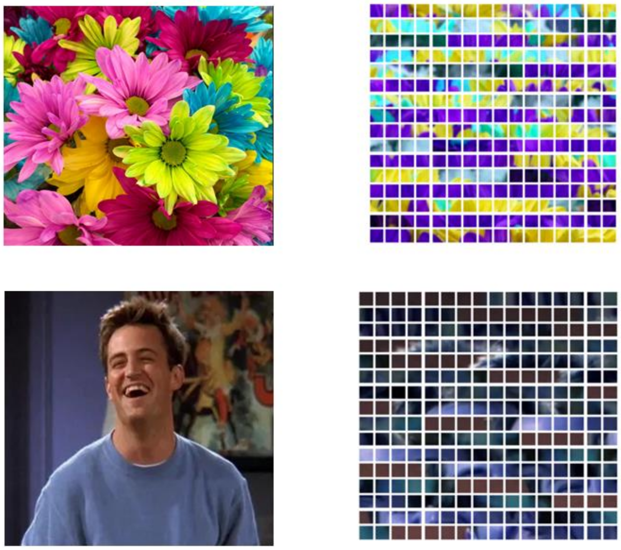

Fig 3. Image before applying quantum walk algorithm and scrambled image after applying the algorithm.

VI. CONCLUSION

The proposed algorithm represent the color image as a quantum state, where each pixel or group of pixels is associated with a quantum state. The algorithm's capacity to handle multiple quantum states simultaneously allows for the secure transformation of each color channel, maintaining the visual quality of the encrypted image. The experimental results show that the randomness of the encrypted image information, key sensitivity, and information entropy effect are good. It can effectively resist statistical analysis attack and differential attack.

ACKNOWLEDGMENT

We extend our heartfelt thanks to the Principal Dr. Yuvaraju B.N and the management and staff of PES Institute and Technology for providing us with necessary insights that enabled us to implement our project. Words cannot describe our gratitude to Dr. Arjun U , HoD, Department of CSE, PES Institute and Technology for his constant support throughout the journey.

REFERENCES

[1] W. H. Yu, "*Research on chaos dynamics of several nonlinear systems*", M.E. dissertation, Xihua Univ., Chengdu, SC, China, 2020.
[2] S. Chen and W. Xue, "*Image encryption algorithm based on chaotic system and artificial neural network*", 2020.
[3] K. Xuejing and G. Zihui, "*A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system*", 2020.
[4] L. Liu, Q. Zhang, and X. Wei, "*A RGB image encryption algorithm based on DNA encoding and chaos map*", 2012.
[5] R.V.Ramos, "*Quantum-Chaotic cryptography*", 2020.
[6] Shihua Zhou, Pinyan He and Nikola Kasabov, "*A Dynamic DNA Color Image Encryption Method Based on SHA-512*", 2020.
[7] Haiju Fan, Heng Lu, Chenjiu Zhang, Ming Li and Yanfang Liu, "*Cryptanalysis of an Image Encryption Based on Random Walk and Hyperchaotic Systems*", 2021.
[8] Yaoqun Xu and Meng Tang, "*Color Image Encryption Algorithm using DNA Encoding and Fuzzy Single Neurons*", 2022. [9] Sitong Liu, Zhichao Lian, Siqi Gu, Liang Xiao, "*Block shuffling learning for Deepfake Detection*", 2022.
[9] Chai, X., Chen, Y., Broyde, L. "*A novel chaos-based image encryption algorithm using DNA sequence operations*", 2017.
[10] Yaoqun Xu and Meng Tang, *"Color Image Encryption Algorithm Using DNA Encoding and Fuzzy Single Neurons",* 2022.
[11] Yi Liu, Gang Cen, Bijun Xu and Xiaogang Wang, *"Color Image Encryption Based on Deep Learning and Block Embedding",* 2022.
[12] Wassim Alexan, Marwa Elkandoz, Maggie Mashaly, Eman Azab and AMR Aboshousha, *"Color Image Encryption Through Chaos and KAA Map",* 2023.