Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 125 (2018) 165–171

Procedia Computer Science

www.elsevier.com/locate/procedia

6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence

Saswat K Pujari[a]*, Gargi Bhattacharjee[b1], Soumyakanta Bhoi[c]

[a]*Tata Consultancy Services, Mumbai, India*
[b]*Department of Information Technology, Veer Surendra Sai University of Technology, Burla, Odisha, India*
[c]*Wipro Technlogies, Hyderabad, Andhra Pradesh, India*

Abstract

With the advent of multimedia technology and rapid data transmission ability of networks, images have become a vital source of extracting information. So its security becomes a critical issue. Images are encrypted to another form in order to preserve their data. In this paper, we have put forward a hybridized model for encrypting images through a combination of Genetic Algorithm and DNA Sequence. DNA sequence is basically chosen as it offers greater storage and higher computing capabilities. The encryption method consists of two phases- Transposition or Scrambling phase and Substitution phase. In the first phase, pixel locations are altered using GA to reduce the correlation among adjacent pixels. In substitution phase, the pixels are replaced by using XOR operation between the pixel values converted into binary strings and DNA substrings derived from a random DNA string. DNA substrings are used as keys for image encryption. The experimental outcome validates that the algorithm is simple, fast enough and feasible. Performance analysis asserts the robustness of the algorithm against all kinds of attacks and thereby maintaining higher security.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications.

*Keywords:*Image Encryption; Genetic Algorithm; DNA Sequence; Meta Heuristic Algorithm; Image Cryptosystem; Image Security.

* Corresponding author.
E-mail address: saswat2603@gmail.com

1877-0509
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications
10.1016/j.procs.2017.12.023

1. INTRODUCTION

The current era has become the epoch of information explosion, thereby making information a crucial strategic resource. So, information security has become a progressively significant task. *Cryptography* is the science of securely transmitting information over a channel. The purpose of this is to safeguard the information from adversaries and make it perceivable solely to the intended recipient. There exists an alternative field referred to as cryptanalysis, which is carried out in parallel to cryptography. The elemental task in cryptanalysis is to analyse and break the protection technique visualized by cryptography. Thus, we can say that 'Stronger the Cryptography, Weaker the Cryptanalysis'. Cryptology encompasses both the fields of cryptanalysis and cryptography [1]. Cryptography serves as a crucial segment of the framework for communication and network security. However, it's been noted that the traditional cryptographic techniques of present day cryptography - like RSA and DES algorithms – possess some latent defects which paved way for attack programs to break it. This observation establishes that present-day cryptographic techniques backed up by mathematical models are not so reliable as before.

Now-a-days, images are used in different processes of information storage and transmission. Therefore, the task of securing and safeguarding image data from unauthorized access is of paramount importance.Image encryption [2] helps prevent disclosure of critical information when they are transmitted over an unsafe channel. First a secret key is selected and using a particular method, the original image is encrypted into the encrypted image, at the sender's end. At the receiver's end, the encrypted image could only be decrypted by the authorized receiver using the secret key to get the original image. Image encryption techniques can be broadly categorized as spatial domain methods and frequency domain methods. The term spatial domain refers to the image plane itself, and all the techniques under this category rely on direct manipulation of pixels in an image. In these algorithms, the conventional encryption typically destroys the correlation among pixels, thereby making the encrypted images incompressible. Frequency domain processing techniques rely on modifying the Fourier transform of an image. Since, it is possible to reconstruct the Fourier transform via an inverse process; we are constantly in need of developing progressively safer and secure image encryption techniques. Image encryption algorithms primarily consist of two steps: Pixel Scrambling and Pixel Substitution [3] [4]. In our proposed work, we've implemented Genetic Algorithm (GA) [5] to realize pixel scrambling and DNA cryptography [6] [7] to realize pixel substitution. GA relies on both substitution and transposition operations. It works on the premise of Darwin's evolution theory. Genetic operation is split into 3 steps: selection, crossover and mutation. The crossover method works similar to the transposition technique and the mutation process like the substitution technique. The study of DNA cryptography-based image encryption algorithms [8] [9] has started gaining prominence in research. The paper has been structured as follows: Section 2 discussing the literature study followed by Section 3 focusing on our proposed method. The following section analyses our results. Finally, the last section concludes our work in addition to highlighting the future extension of this topic.

2. LITERATURE SURVEY

In 2011, Amitava Nag et.al [11] applied affine transformation to decompose an image into 2*2-pixel block size, and afterwards, applied a XOR operation on each block with four sub key of 8 bits to produce a cipher image. But the algorithm is less effective in reducing the correlation between pixels and also has short key space. In 2012, Long Bao and Yicong Zhou [12] suggested a chaotic system that uses one- dimensional chaotic maps and the Substitution-Permutation Network (SPN) to obtain confusion and diffusion property. It uses a 240-bit key containing all parameter settings and excessive sensitivity in key changes for encryption and decryption. Amnesh Goel and Nidhi Chandra [13] put forward a technique that uses a transformation algorithm consisting of two stages to minimize the correlation between pixels. At the first stage, the algorithm performs horizontal block displacement followed by the vertical block displacement. Thereafter, in the second stage, the technique performs inter pixel displacement of RGB values. Mohammed Abbas and Fadhil Al-Husainy [14] contrived an approach relying on bit level permutation that utilizes two Boolean operations: XOR and Rotation on the bits of the pixels to satisfy the confusion and diffusion properties. Furthermore, to encrypt an image, the algorithm applies a sequential XOR