Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 3, March 2021, pp. 1455~1464
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i3.pp1455-1464

A novel image encryption scheme based on DCT transform and DNA sequence

Ali A.Yassin[1], Abdullah Mohammed Rashid[2], Abdulla J. Yassin[3], Hamid Alasadi[4]
[1,3,4]Computer Science Department, Education College for Pure Science, University of Basrah, Basrah, Iraq
[2]Education College for Human Science, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Oct 10, 2020
Revised Dec 7, 2020
Accepted Dec 23, 2020

Keywords:

Cryptanalysis
DCT transform
DNA sequence
Image encryption

ABSTRACT

Recently, the concept of DNA has been invested in computing technology in different ways which linking information technology and biological sciences. However, the DNA encryption scheme has drawbacks such as expensive experimental equipment and hard to hold its biotechnology. Additionally, during careful cryptanalysis that applied to most of these image encryption schemes, we notice that DNA can only influence one DNA base, which causes poor diffusion. Our proposed scheme is not applied complex biological operation but just is given to improve the diffusion ability of image encryption scheme by using DNA sequence and DCT transform. Furthermore, empirical results on real images and security analysis demonstrate that our scheme not only has flexibility and efficiency encryption scheme but also has the ability to resist well-known attacks such as entropy attack and statistical attack. Additionally, our work enjoys several strong characteristics as follows: (1) the decryption error is very low to recover the original image; (2) Once key for each encryption process and if the user wants to use the same key in many times, our scheme supports secret key sensitivity; (3) the value of correlation of the encrypted image is null.

Corresponding Author:

Abdulla J. Yassin
Computer Science Department
Education College for Pure Science
University of Basrah. Iraq 42001
Email: abdullajas@uobasrah.edu.iq

1. INTRODUCTION

In the last years, the communication and network systems have been changed due the information technology and Internet. At the present time, ten-thousands of kilobytes of trusted information are transferred in Internet over insecure communication channels, the information may be exposed to interrupting by an adversary that tries to obtain or change information. The protected communication method is that an user (sender) encrypts the original image in to encrypted image based on certain encryption method and only the legal receiver has ability to decrypt the encrypted image with the secret key(s) to retrieve the sender's image. There are many mainly schemes for image encryption such as diffusion (by using pixel replacement), permutation (by using pixel scrambling), or both diffusion and permutation. Furthermore, we find several applications of image encryption in many fields such as video conference, military, biometric systems, personal image. These applications require strong encryption scheme that has a good balanced between security and performance. There are several studies appear recently used DNA in cryptography [1-3].

Conversely, several image encryption schemes have been presented for both gray image and real image, for instance, partial encryption, DNA cryptography, transform domain, and modern cipher text but