ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

A Novel Image Encryption Technique with Four Stage Bit-Interspersing and A 4D-Hyperchaotic System

Subhashish Pal[1], Ansuman Mahanty [2], Arghya Pathak[3], Jayashree Karmakar[4],
Hrishikesh Mondal [5] and Mrinal Kanti Mandal[6]

ABSTRACT

This paper introduces a new technique of color image encryption that includes four stages of bit interspersing and a 4D-hyperchaotic system. At first, the pixel values for different RGB channels of a plane color image were represented by an 8-bit binary number. The bit interspersing operation has been implemented on the bit stream generated by considering a particular block size for each color channel and reshaping it to the original size. The cipher image was then constructed by performing a bit XOR operation on the resultant image and the chaotic sequences generated by a 4D hyperchaotic system. The initial state variables of the said chaotic system have been developed from a 32-character secret key. This operation has been repeated three times, considering different block sizes of the newly generated cipher image after each stage. The main strengths of the proposed algorithm are the bit interspersing and image-dependent chaotic key base pixel substitution by bitwise XOR operation. A set of standard security tests are conducted to test the reliability of the suggested encryption method. Comparing the crypto-parameters to other recent works, we find that the proposed algorithm is better than the other methods.

Article information:

Keywords: Bit interspersing, Cryptography, Chaos, Hyperchaotic system, Encryption, Decryption

Article history:
Received: August 29, 2022
Revised: December 9, 2022
Accepted: January 21, 2023
Published: March 4, 2023
(Online)

DOI: 10.37936/ecti-cit.2023171.249733

1. INTRODUCTION

The growth of the internet and communication infrastructure has increased the volume and variety of shared data, making it more difficult for cryptosystem designers to guarantee the privacy of transmitted information. Many researchers have reported essential contributions to data security. Cryptography is a subset of data security systems that encrypts data before sending it across a network so that only the intended recipient can decipher it. In cryptography, keys are essential tools for encrypting and decrypting information. When both the keys are the same, that type of encryption is termed symmetric key cryptography, and if they are different, it is called asymmetric key cryptography [1].

In modern cryptography, the encryption algorithm plays a pivotal role in determining the quality of the cryptosystem. The more complex the encryption algorithm leads to a robust cryptosystem against attacks. In the last two decades, chaos-based cryptography [2] has drawn the attention of researchers as the pseudorandom sequences produced by such nonlinear chaotic systems are hard to understand and anticipate because of their structural complexity. Stochasticity, sensitivity to their beginning circumstances, and control parameters contribute to their popularity in such applications. As far back as 1998, Fridrich came up with the concept of chaotic encryption [3]. Permutation and diffusion are the two main components working behind such designs; hence, many cryptography researchers prefer chaotic systems [4]. In the last few years, using hyperchaotic systems in cryptography has become more popular than a standard chaotic system. Hyperchaotic systems are those chaotic systems that have more than one positive

[1,3,6] The authors are with Department of Physics, National Institute of Technology, Durgapur 713209, India, E-mail: sp.20ph1501@phd.nitdgp.ac.in, ap.18ph1102@phd.nitdgp.ac.in and mrinalkanti.mandal@phy.nitdgp.ac.in

[1,2] The authors are with Department of Physics, Dr. B. C. Roy Engineering College, Durgapur 713206, India, E-mail: subhashish.pal@bcrec.ac.in and ansuman.mahanty@bcrec.ac.in

[4] The author is with MUSE Lab, Indian Institute of Technology, Gandhinagar-382355, India, E-mail: jk.16ph1102@phd.nitdgp.ac.in

[5] The author is with Department of Physics, Durgapur Government College, Durgapur 713214, India, E-mail: hm.13ph1505@phd.nitdgp.ac.in