International Research Journal of Engineering and Technology (IRJET) e-ISSN: 23950056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A Secure and High-Capacity Data-Hiding Method using Arnold Transform and Chaotic Scrambling

K.B Loganathan[1], M Kishor[2], C Muniyappan[3], Dr.S Karthigai Lakshmi[4]

[1,2,3]*Under Graduate student, ECE Department, SSMIET, Dindigul, Tamil Nadu, India*
[4]*Associate Professor, ECE Department, SSMIET, Dindigul, Tamil Nadu, India*

***

Abstract: *In the fast growing digital world, the protection and transmission of data securely is becoming huge challenge through an open medium like internet. There are several methods for information security process like Cryptography and Steganography. The different data hiding method are lossless compression, advanced encryption standard (AES), modified pixel value differencing (MPVD), and least significant bit (LSB) substitution is presented. In the lossless compression, Arithmetic coding was applied on a secret message to provide 22% higher embedding capacity. The hidden message which is compressed is then given to AES encryption for better security. After compression and encryption, the LSB substitution and MPVD are applied in this work. The proposed scheme is composed of Arnold scrambling and chaotic scrambling (SC-HAC).The security is considered by the proposed scheme which combines Arnold scrambling and Logistic scrambling to improve the encryption effect. Here, Arnold transform and chaotic scrambling is used to increase the SSIM value for better quality of compressed image.*

Keywords: Arnold Transform, chaotic scrambling, encryption, decryption, cover image, Digital Image Processing, Steganography, chaos, Reversible data hiding, absolute moment block truncation coding (AMBTC).

1. INTRODUCTION

Steganography is method of hiding information in which prevent the detection of hidden messages and this can be achieved by hiding information inside another piece of innocent looking information. The different embedding methods are the spatial, time domain methods, Transform domain methods, etc. These methods hide/embed information in numerous kinds of media like text, image, audio, video etc. Among these types of different file formats, digital images are considered to be the foremost popular style of carriers due to their size and distribution frequency. Covert or hidden communication is that the process of hiding data in another information. There are many hidden communication techniques such as, Cryptography, Steganography, Covert channel, Watermarking etc. Steganography is the effective means of information or data hiding that protects information from unauthorized disclosure. It works by hiding secretive information into ordinary and innocent looking messages those are generally out of suspicion.

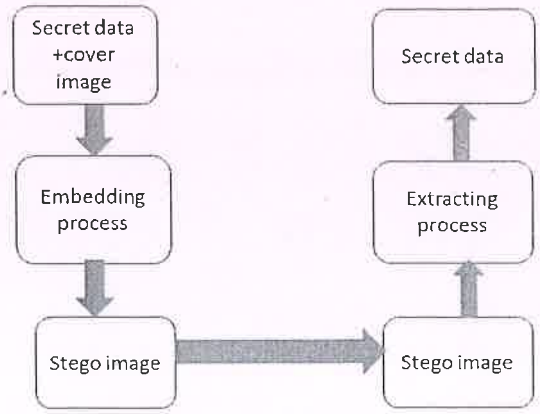

Fig.1 General Structure

The proposed system has following methods; they are embedding phase and the extraction phase. Within the embedding phase, the secretive message is first scrambled using transform at different levels, to create it safer against unauthorized extraction. This scrambled message is embedded into the cover image to get the stego image .then the stego image is transmitted and at the receiving end the hidden secret message is extracted by following the extraction and decryption process within the reverse order. During this technique, the values are kept secret and are only known to the authorized users and extraction without the keys results with noises, making the procedure secure.

2. STATISTICAL ELEMENTS

2.1 Mean:

Mean value gives the contribution of each pixel intensity for the whole image & variance is normally used to find how every pixel varies from the nearby pixel .The mean gives an idea where your pixels are (i.e. are they black, white, 50% gray,). The mean will give you an idea of what pixel color to choose to summarize the color of the complete image