ABSTRACT

Internet is an important entity in the daily life of people in many ways, which allows people in different parts of the world to share all types of information. Information security is a vital issue for data storage and exchange of sensitive digital data through Internet. The need for data privacy and security has become essential in telecommunication because of increased security threats.

Cryptography provides an effective solution for securing data communications over the public networks. Transmission of multimedia data over the Internet has increased due to the development of simple and easy to use digital communication techniques. Among the different types of multimedia data, images are transmitted very often due to their wide usage in different applications. In fields like medicine, defence, space, education, and other industrial domains, massive amount of information are gathered, stored, and transferred in the form of digital images.

Data security is an inevitable issue because of the variety of software and hardware vulnerabilities present in the network. Thus, it is essential to protect the sensitive image data from unauthorized disclosure. The traditional and pioneer cryptosystems like Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA) are the frequently used algorithms to encrypt textual data. The algorithms that are good for the encryption of textual data are not suitable for the encryption of multimedia data due to large data size and execution time constraints. Image encryption is a technique used to share sensitive image information through insecure networks with confidentiality.

Based on permutation the image encryption methods are classified as bit permutation, pixel permutation, and block permutation. In bit permutation, the bits of each pixel of the image are permuted with the key chosen from a set of keys. In pixel permutation, the pixel position of the image is rearranged using the key selected from a set of keys. In the case of block permutation, the image is divided into blocks and these blocks are permuted based on a random key.

Typically, pixel permutation based image encryption methods use scan patterns for image scrambling. Scan pattern is a formal language-based two dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths. Primarily, random number is used to offer substitution by using the simple and efficient bitwise XOR operation. Good cryptographic techniques require good random numbers, and hence, the random numbers play an important role in image encryption. In general, diffusion is achieved by repeatedly performing several permutations and confusion is achieved by substitution.

The objective of this research is to develop certain simple and effective image encryption methods using scan pattern based pixel permutation and random number. In image encryption, bitwise XOR operation is used to replace a pixel value with another pixel value to provide confusion property. To implement this, random numbers are mainly used in image encryption.

In this research, six new scan patterns for pixel permutation, two methods for generating random key stream, and a method to generate true random numbers are proposed.

In the proposed work, the following are the six new scan patterns generated by using certain novel concepts. The concept of Matrix Reordering (MR) provides well permuting rows and columns of a matrix. In the proposed method, the pixel permutation has been carried out by using scan patterns

developed from the concept of Matrix Reordering (MR). The concept of Z-order Curve (Z-oC) and Hilbert Curve (HC) has been used for generating sequence of one-dimensional numbers for indexing in storage and retrieval of multi-dimensional data. In this research, the above said concepts are used as scan patterns for pixel permutation. The idea used for locating the K^{th} smallest element in a randomly ordered array is utilized to generate scan pattern for pixel permutation. The Knight's Travel Path (KTP) is a pattern in which the path of a Knight around a chess board is taken without revisiting any node. In this research, a new scan pattern for pixel permutation is generated by using the Knight's travel path. Calligraphy is an art of generating the symbols of a language. In this research, the calligraphy technique is used to generate a new scan pattern for pixel permutation.

The proposed work includes two new methods to generate random key stream by adapting the randomized bit pattern generation used for MD5 and SHA-512 hash functions and introduces a method for generating true random numbers from the sampled amplitude value of an audio signal.

The performance of the proposed image encryption methods is tested with standard gray-scale images and analyzed using the evaluation metrics like histogram, correlation coefficient, randomness test, information entropy, noise attack test, key space, and execution time. It is found that the developed image encryption methods are comparatively simple, takes less time for encryption, and provides a significant improvement in securing data storage and transmission.