ABSTRACT

The goal of image cryptosystems is to protect image transmission when there are network adversaries present. To ensure secrecy, images are subject to encryption to produce unintelligible cipher images; the techniques used for this process differ significantly from those applied to text data. The majority of the cryptosystem consider complicated or confusion–diffusion architectures that changes and permute the values of the pixels. Their aim is to make the relation between key and text as complex as possibleand to propagate every text knowledge to the entire system. These frequently entail binary operations like bitwise XOR, plus–minus, DNA operations, etc; are carried out utilising chaotic maps, each of which have certain limitations. This thesis employs a binary function that can be applied to both traditional and DNA techniques for coloured natural images, and can be applied to any kind of image cryptosystem. Each of the color component of the image follows some steps which start with inter channel mixing and mix rows which takes the value from initial vector and mixes it with the first element of every row and propagates its value to the entire row operating wth the suggested operator , then Arnold cat map algorithm is applied to shuffle the pixels. Secondly spiral mixing of the pixel is applied in four different directions viz. forward row and column, backward row and column to prevent differential attack. Finally, encoding, substitution, and decoding based on DNA is carried out. A multiple collapse chaotic map is used to derive initialization vector, rule charts and DNA substitution map which are used in encoding and decoding processes. Analysis and experimental findings shows that our cryptosystem has significant performance and different metrics shows it can withstand different type of attacks. Comparative analysis with modern cryptosystems demonstrate the acceptable performance of our cryptosystem.