CHAPTER 3

PROPSED METHOD AND TOOLS

3.1 Overview:

One of the most important symmetric cryptographic algorithms is Rivest Cipher 4 (RC4) stream cipher which can be applied to many security applications in real time security.

RC4 design avoids the use of Linear Feedback Shift Registers (LFSRs) where many stream cipher algorithms depend on it, especially in hardware. it attempts to achieve highest randomness via swapping of elements in arrays. The RC4 algorithm has variable key length which ranges between 0 to 255 bytes for initializing 256-byte array in initial state by elements from S [0] to S [255] [13].

3.2 Digital Images:

Digital image is a representation of two dimensional image using ones and zeros (binary).

Digital image in the computer is an array of numbers that represent light intensities at various points (pixels).

3.2.1 Type of Digital Images:

- **A binary image** is a digital image that has only two possible values for each pixel. Typically, the two colors used for a binary image are black and white (0, 1).
- **Grayscale image** is an image in which the value of each pixel represent also as black-and-white, are composed exclusively of shades of gray, varying from black and white.

- **Color images** are stored in either 24-bit (true color images) or 8-bit per pixel files. A common image size is 640 × 480 pixels and 256 colors (or 8 bits per pixel) Represent colors RGB.

3.3Image Encryption Techniques:

- Image encryption using affine transform and xor operation.
- Anovel digital image encryption method based on one-dimensional random scrambling.
- A technique for image encryption based on explosive n*n block displacement followed by inter-pixel displacement of attribute of a pixel.
- Anovel neural network approach for digital data encryption/decryption.
- Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location.

3.4 Research Methods:

3.4.1Standard RC4 Method:

The standard RC4 algorithm has many step to implement encryption and decryption process.

- Vector initialization: in this step two 256 byte vectors are initialized, state vector S with values from 0 through 255 in ascending orders. Temporary vector T with values from user selected master key k.
- Key Scheduling Algorithm (KSA) an initial permutation of S is carried out based on the temporary vector T, after KSA the master key (K) and temporary vector (T) are discarded.
- Pseudo Random Generator Algorithm (PRGA) the algorithm cycles through the values of S from S [0] to S [255] to produce the pseudo random byte key stream .after each byte key (k) is generated, the vector S is subjected to another permutation as per the current state of S.

For encryption process XOR operation is generated of each byte of plain (p) with corresponding byte key to generate the cipher (C).

For decryption process XOR operation is generated of each byte of cipher (C) with corresponding byte key to generate the plain (p).

3.4.2 Enhanced RC4 Method:

In enhanced RC4 algorithm method the main steps of standard RC4 used in addition to new process to some steps as following:

- In key Scheduling Algorithm (KSA) step the state1 is permuted with state2, then state1 is added and XORed with temporary key state the result of this process is new permuted state1.
- In Pseudo Random Generator Algorithm (PRGA) the permuted state1which is XORed with permuted state2 to generate key stream in pseudo random number generator is XORed with original image to produce cipher image.

3.4.3 Flow chart of Enhanced RC4 Process:

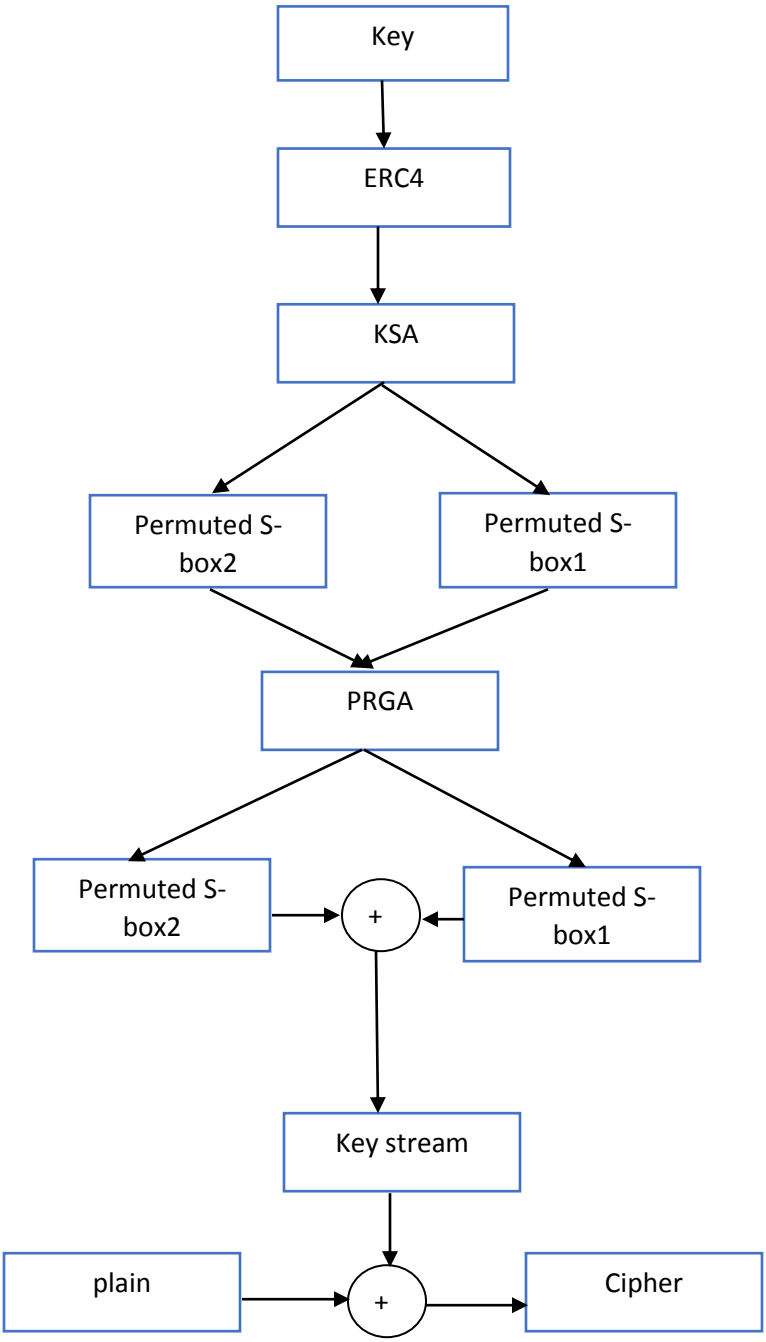

Figure 3.1 Flow chart of basic operation of encryption process by ERC4.

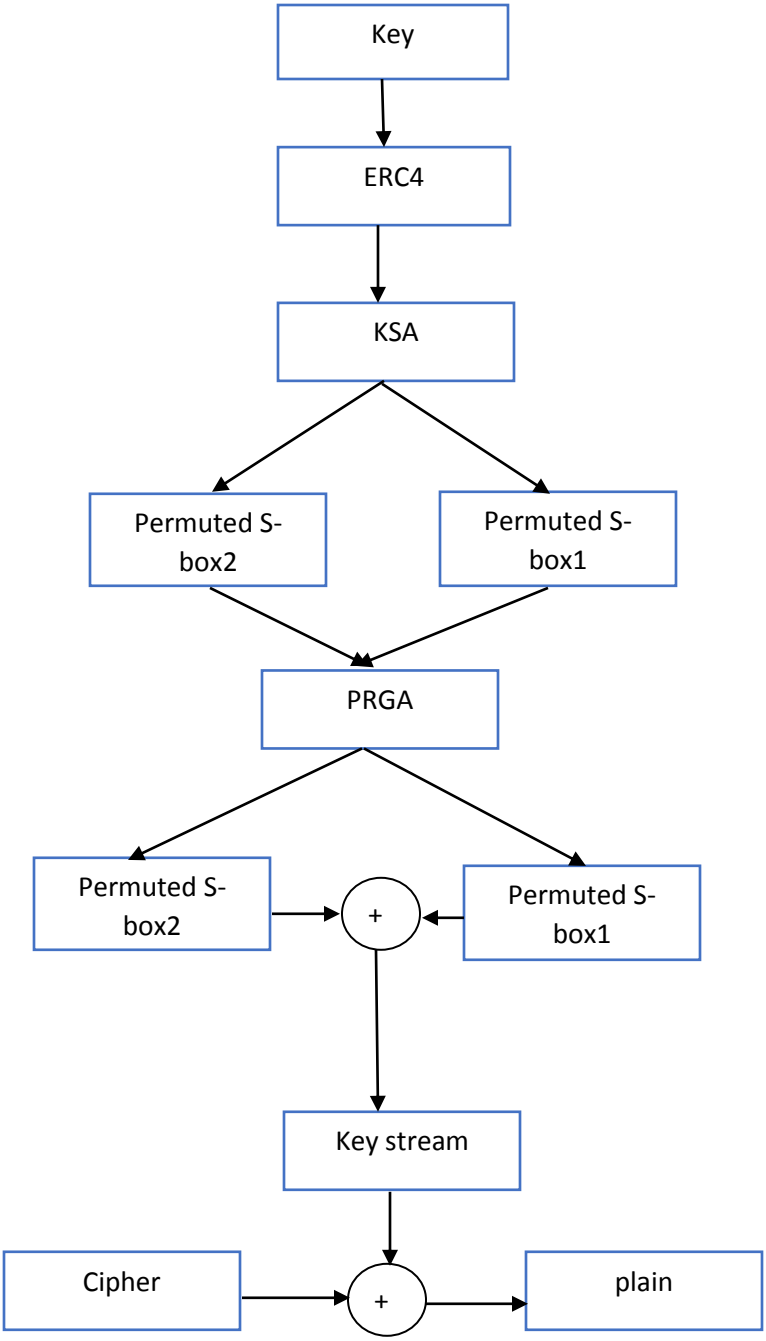

Figure 3.2 Flow chart of basic operation of decryption process by ERC4.

3.5 Algorithm Performance:

Performance evaluation is very important part in the any algorithmic design in encryption.

To measure efficiency the system performance by calculating the following parameters:

3.5.1 Mean Square Error (MSE):

The mean squared error (MSE) is used to estimate or measures the average of the squares of the "errors", between original image and decrypted image.

MSE is then calculated as follow:

MSE=(im1-im2)/image size

3.5.2 Peak signal to Noise ratio (PSNR):

Peak Signal to Noise Ratio (PSNR) is used to determine the efficiency of encryption with respect to the noise.

The noise will degrade the quality of image. the visual quality of original images and decrypted images is measured using the Peak Signal to Noise Ratio [14].

In PSNR, we take the square of the peak value in the image (in case of an 8 bit image, the peak value is 255) and divide it by the mean square error.

The PSNR is then calculated As follows:

PSNR =10 log (P2 / MSE).

Where:

P= maximum value in original image.

3.5.3 Randomness Test:

A random bit sequence could be interpreted as the result of the flips of an unbiased "fair" coin with sides that are labeled "0" and "1," with each flip having a probability of exactly ½ of producing a "0" or "1." Furthermore, the flips are independent of each other: the result of any previous coin flip does not affect future coin flips.

The need for random and pseudorandom numbers arises in many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols [15].

3.5.4Random Number Generation Tests:

The NIST Test Suite is a statistical package consisting of 15 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence [16].

3.5.5 The Frequency (Mono-bit) Test:

This test tests the uniform distribution of the values generated by a pseudorandom number generator. An attempt is made to identify any deviations from a uni-dimensional uniform distribution [17]. this entails checking the number of zeros and ones in sequence *s* against the expectation that if the sequences were genuinely random, one would expect the numbers of zeros and ones to be virtually the same .in this research this test done by using CrypTool.

3.5.6 Diehard Tests:

The diehard tests are a battery of statistical tests for measuring the quality of a random number generator. They were developed by George Marsagliaover several years and first published in 1995 on a CD-ROM of random numbers [18].

3.5.6.1Runs Test:

Generate a long sequence of random floats on (0, 1). Count ascending and descending runs. The counts should follow a certain distribution[18].

3.5.6.2 Count the 1's in specific bytes Test:

This is test count the 1 bits in each of either successive or chosen bytes. Convert the counts to "letters", and the count occurrences of five-letter "words" [18].

3.5.6.3Overlapping sums test:

This is test a long sequence of random floats on (0, 1). Add sequences of 100 consecutive floats. The sums should be normally distributed with characteristic mean and variance [18].