CHAPTER 4

RESULTS AND DISCUSSION

4.1 Simulation Environment

4.1.1 Java:

Java is general purpose computer programming Language that is concurrent, class-based, object-oriented and specially designed to have as few implementation dependencies as possible.

Sun microsystem released the first public implementation as Java 1.0 in 1995.it promised "Write Once, Run Anywhere" (WORA), providing no-cost run-times on popular platforms [12].

4.1.1.1 Significant Language Features:

Simple: Java is an extension of C and C++ with added feature of garbage collection and improved memory management**.**

Object-oriented: Object oriented programming deals with objects and there behaviors and hence an analogy of real world can be found in programs.

Network-savvy: Java has an extensive library of routines for coping easily with TCP/IP protocols like HTTP and FTP. This makes creating network connections much easier

Robust: Java is intended for writing programs that must be reliable in a variety of ways. Java puts a lot of emphasis on early checking for possible problems, later dynamic (runtime) checking, and eliminating situations that are error prone**.**

Secure: Java is intended for use in networked/distributed environments. toward that end, a lot of emphasis has been placed on security. the changes to the semantics of pointers make it impossible for applications to forge access to the user's hard disk.

Architecture neutral: To enable a Java application to execute anywhere on the network, the compiler generates an architecture-neutral code – byte code which is executable on many processors, given the presence of the Java runtime system.

Portable: There are no "implementation dependent" (machine/ processor dependent) aspects of the specification. The sizes of the primitive data types (integer, float) are specified**.**

Interpreted: Java byte codes are translated on the fly to native machine instructions (interpreted) and not stored anywhere.

High performance: Java Byte code is more efficient and its interpreted nature provides high performance.

Multithreaded: Multithreading is a way of building applications with multiple threads (more than one processes running at the same time). It is useful for better interactive responsiveness and real-time behavior**.**

Dynamic language: Java programs carry substancial amount of run time information.

4.1.2 MATLAB:

MATLAB is widely used in all areas of applied mathematics, in education and research at universities, and in the industry. MATLAB stands for Matrix Laboratory and the software is built up around vectors and matrices. This makes the software particularly useful for linear algebra but MATLAB is also a great tool for solving algebraic and differential equations and for numerical integration. MATLAB has powerful graphic tools and can produce nice pictures in both 2D and 3D. It is also a programming language, and is one of the easiest programming languages for writing mathematical programs. MATLAB also has some tool boxes useful for signal processing, image processing, optimization, etc. [13].

4.2 Image formats supported by Java:

- JPG
- BMP
- PNG
- TIFF
- GIF
- PSD

4.3 Flow chart of image encryption and decryption process:

The following flow chart explain the encryption and decryption process in enhanced RC4 algorithm.

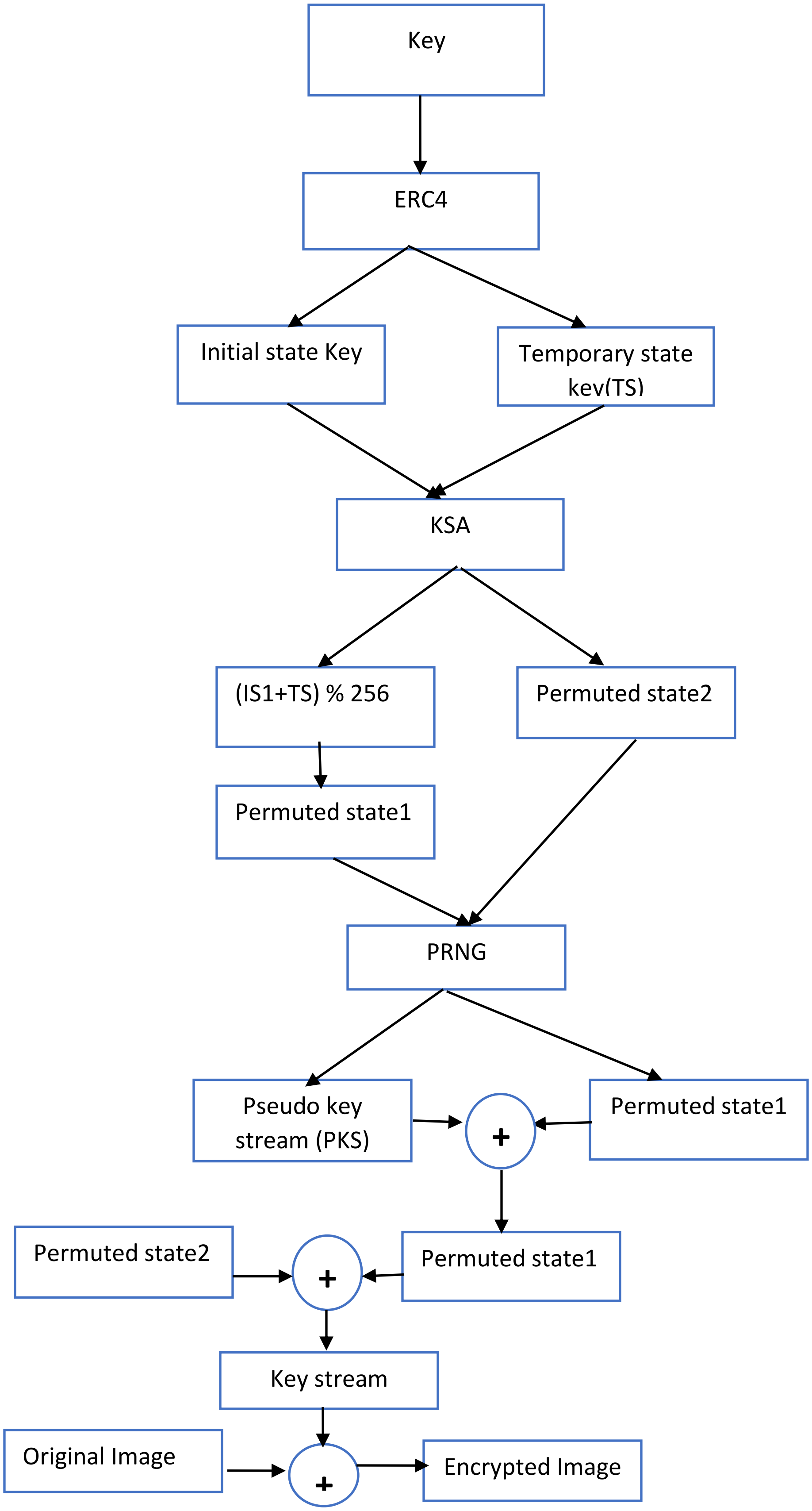


Figure 4.1 Flow chart of Image encryption

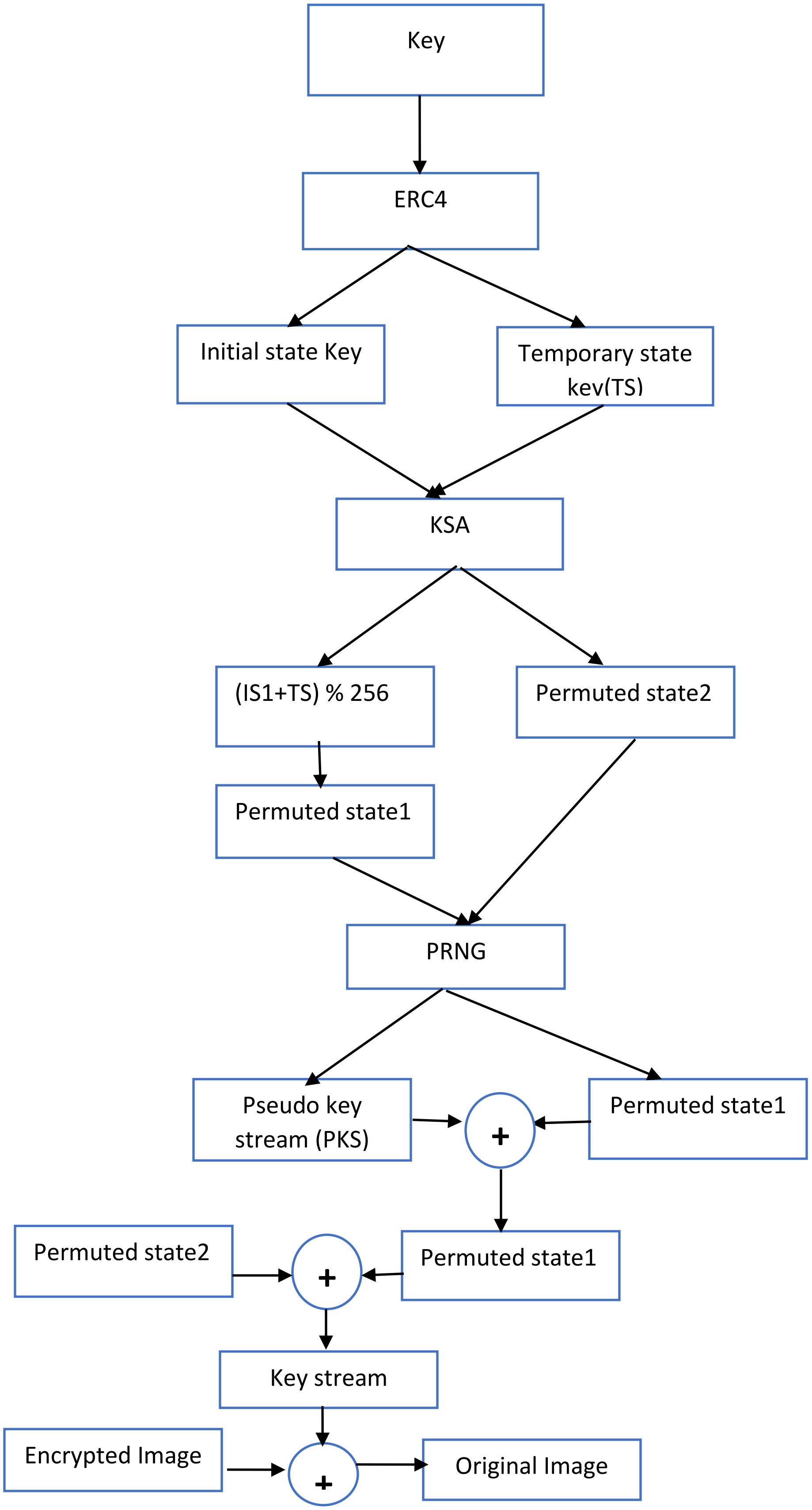


Figure 4.2 Flow chart of Image decryption

The above flow chart describe image encryption and decryption process using enhanced RC4 algorithm, the encryption and decryption process is divided to following steps:

- Key scheduling algorithm: is first step to generate permuted state1 as result of combination of initial state and temporary key state.
- Pseudo random number generator: the input of this state permuted state1 and pseudo key stream, the two input is added and XORed to generate new permuted state1 that is XORed with permuted state2, the result is key stream which is XORed with original image to generate cipher image.
- We use the same steps for encryption and decryption process.

4.4 MSE AND PSNR:

The Enhanced RC4 algorithm can accept images in different formats and different sizes.

To ensure that is quality of image cannot effected by decryption process we use MSE and PSNR value. MSE Calculate the difference between the two images, if the value of MSE small it means good result.

The PSNR is used to measure the quality of an image after the reconstruction. The big value of the PSNR it means the result is so good.

Table 4.1 The results of MSE and PSNR value.

Original Images	Decrypted image	MSE	PSNR
 (a)	 (1)	0.00	Inf
 (b)	 (2)	0.00	Inf
 (c)	 (3)	0.00	Inf

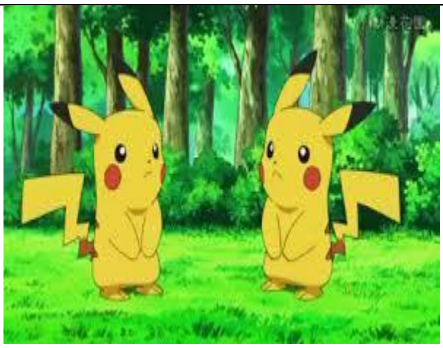
The images (a,b,c) represent the original image before encryption process where images (1,2,3) represent decrypted image , we use MSE to calculate the different between two images after that we calculate the PSNR value .

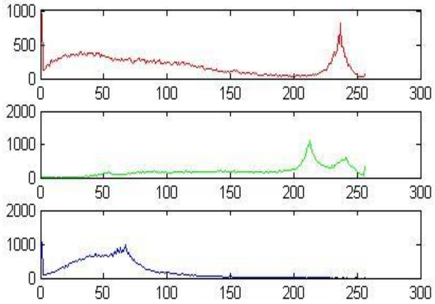
4.5 Histogram:

Histogram is a representation of the distribution of colors in an image. For digital images, a color histogram represents the number of pixels that have colors in each of a fixed list of color ranges that span the image's color space, the set of all possible colors.

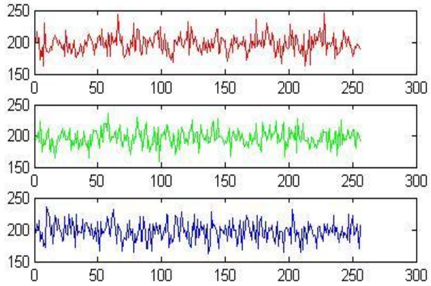
In the histogram form image properties tested three colors (RGB).

Table 4.2 show the result of images and histogram.

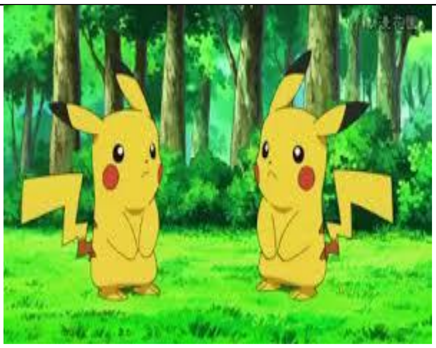
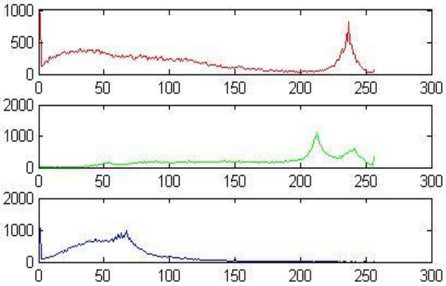
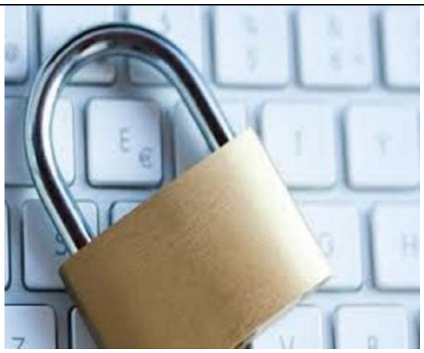
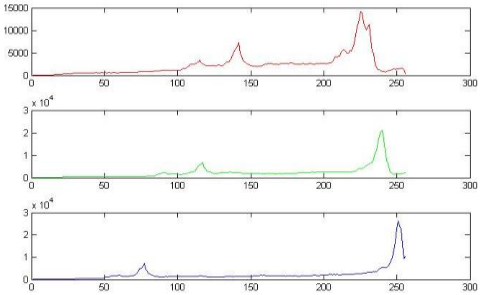
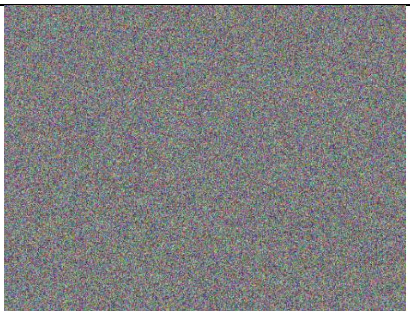
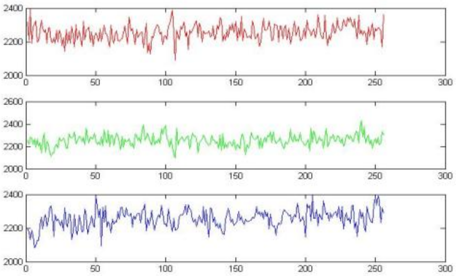
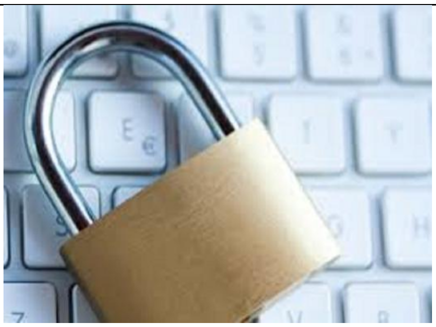
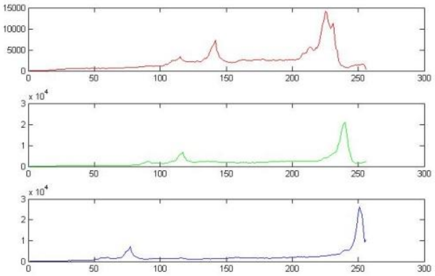
<table>
<tr><th>Different Images</th><th>Histogram</th></tr>
<tr><td>


(a)
</td><td>


(1)
</td></tr>
<tr><td>

(b)
</td><td>


(2)
</td></tr>
</table>

 (c)	1000 500 0 0 50 100 150 200 250 300 2000 1000 0 0 50 100 150 200 250 300 2000 1000 0 0 50 100 150 200 250 300 (3)
 (a)	15000 10000 5000 0 0 50 100 150 200 250 300 x 10^4 3 2 1 0 0 50 100 150 200 250 300 x 10^4 3 2 1 0 0 50 100 150 200 250 300 (1)
 (b)	2400 2200 2000 0 50 100 150 200 250 300 2600 2400 2200 2000 0 50 100 150 200 250 300 2400 2200 2000 0 50 100 150 200 250 300 (2)
 (c)	15000 10000 5000 0 0 50 100 150 200 250 300 x 10^4 3 2 1 0 0 50 100 150 200 250 300 x 10^4 3 2 1 0 0 50 100 150 200 250 300 (3)

In table (4.2) Image (a) represent the original image before encryption process and figure (1) is histogram of image(a) , after image(a) is encrypted the result is image (b) that is difference from original image and figure(2) is histogram of image (b) ,the result of decryption process image (c) that is similar to image(a) and figure(3) and figure(1) are similar.

4.6 Randomness Tests:

The randomness of algorithms is measured using crypto tool 1.4.31 beta and different Significance level alpha, the result of the test is shown in the following table

Table 3.4 Result of frequency test between enhanced RC4 and standard RC4.

Test Name	**Significance level alpha**	**ERC4 Test result**	**Status**	**RC4 Test result**	**Status**
Frequency	**0.05**	**3.755278**	**Passed**	**3.201260**	**Passed**

The above table show the result standard RC4 and enhanced RC4 algorithm after doing frequency test by using crypTool.

Also the randomness of algorithm is measured using diehard testing tool, the result of test is shown in the following table.

Table 4.4 Result of Diehard Tests between enhanced RC4 and standard RC4.

Tests	**Standard RC4**	**Enhanced RC4**	**Status**
COUNT-THE-1's TEST for specific bytes	Byte1 Chi square= 466526.300 Byte 8 Chi square= 466722.300	Byte1 Chi square= 460717.200 Byte 8 Chi square= 460606.500	**Passed**

OVERLAPPING SUMS test	p-value =1.000000	p-value =1.000000	**Passed**
RUNS test	runs up; ks test for 10 p's:.476105 runs down; ks test for 10 p's:.660969	runs up; ks test for 10 p's: .936613 runs down; ks test for 10 p's: .504526	**Passed**
Second time Run time	runs up; ks test for 10 p's: .999980 runs down; ks test for 10 p's: .999917	runs up; ks test for 10 p's: .040859 runs down; ks test for 10 p's: .801363	**Passed**

The passed Tests indicates the p's value is acceptable and has good randomness, where the failure mean the sequence is not acceptable due to non-randomness.

count-the-1's test for specific bytes for sample size=256,000 ,in standard RC4 result Byte1 Chi square=466526.300 is greater than result in enhanced RC4 with value= 460717.200 that is mean the number of 1's in specific byte in enhanced RC4 is more randomness than standard RC4.

The result of run test in standard RC4 in runs up for first run test with value .476105 is better than enhanced RC4 with value .936613 depend on the sequence of length 10,000 and the time of run test.

But the results of run test in enhanced RC4 in runs down for first run test with value .504526 is better than standard RC4 with value .660969depend on the sequence of length 10,000 and the time of run test.

In second time run test the runs-up and runs-down results of enhanced RC4 is better than standard RC4 depend on the sequence of length 10,000 and the time of run test.