CHAPTER 1

INTRODUCTION

1.1Overview:

The increase use of the electronic communication demands more and more security on the exchange of the critical information.

Cryptography now a day's get more and more importance to address this issue.

The cryptography allows two people to exchange a message in such a way that other people cannot understand the message.

"The encrypted data is sent over the public network and is decrypted by the intended recipient.encryption works by running the data through a special encryption formula. both the sender and the receiver know this key which may be used to encrypt and decrypt the data "[1] .

Encryption provides an obvious approach to information security and encryption programs are readily available. encryption algorithms available for textual data are highly efficient. but sometime the information is available in form of image. in such cases we need a specialized algorithm that is highly optimized to protect pictorial information.

RC4 is the most widely used stream cipher in the world. It is used in protocols like SSL, WEP, WPA, and applications like Skype, Remote Desktop and Microsoft Point-to-Point. There are many other applications which use RC4 as the encryption algorithm. It is used in hardware based encryption mechanisms as well. Due to its light weight it has become popular [2].

1.2 Problem Statement:

In cryptography, RC4 is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) to protect internet traffic and WEP to secure wireless networks. while remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems.it is especially vulnerable when the beginning of the output key stream is not discarded, nonrandom or related keys are used, or a single key stream is used twice; some ways of using RC4 can lead to very insecure cryptosystems such as WEP [2].

In this research two state tables are used to solve correlation problem between the public known output of internal state by using permutation between state1 and state2 that is improve the RC4 algorithm.

1.3 Research Objectives:

- To make RC4 algorithm more strong for image encryption and decryption process.
- To solve correlation problem between the public known output of internal state by using permutation between state1 and state2.

1.4Methodology:

In this research the enhancement of RC4 algorithm done by using two state tables and use different key length byte instead of 256 byte to make algorithm strong and used it for images encryption and decryption.

- first in key Scheduling Algorithm(KSA) step the state1 is permuted with state2 , then state1 is added and XORed with temporary key state .
- Second in Pseudo Random Generator Algorithm (PRGA) the result of first step is new permuted state1 which is XORed with permuted state2 to

generate key stream which is XORed with original image to produce cipher image.

- The Implementation of the system done by using java programming language.
- MATLAB is used to analysis the performance by calculating the Mean Square error (MSE) and Peak Signal to Noise Ratio (PSNR) that Parameters used to measure the quality of the image.

1.5 Research scope:

Research activities in enhancement of algorithms have become more active research area.

In our research we select stream cipher RC4 as improvement algorithm .In this research area there are many proposed method to implement to RC4 algorithm.

The areas that contribute to the development of image encryption include the following:

- Cryptography.
- Digital image Processing.

Each of these areas deals with a particular aspect of the image encryption process.

1.6 Thesis out line:

This research is organized as **5** chapters:

- Chapter (1) overview of the research topic and problem statement and research objectives.
- Chapter (2) Literature review and Related work.
- Chapter (3) Proposed Method and Tools.
- Chapter (4) Results and discussion.
- Chapter (5) Conclusion and Recommendation.