Chapter - I

INTRODUCTION

1-1 Introduction

Images are one type of data that can contain valuable information. Currently, many users are transferring and exchanging image files across the internet. These images may include photos, maps, scanned document, etc. It became easy for intruders to intercept these files while it is being transferred or even while it is stored on local storage. Securing such files has been necessary and required to protect the information even if it fell in the wrong hands.

Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable to image and multimedia applications because of large data sizes and real time constraint. Heavy weight encryption and decryption algorithms will aggregate the problem and increase the latency. Security is a trade-off between the cost of the data being protected and the cost it takes an attacker to get the data. Protecting data worth only several dollars with security system that costs a million dollars to break is obviously a bad investment. The trade of is to find the balance between the cost to an attacker and the value of the data to its owner. The cost to break a security system can be measured in many ways, which include the amount of computer time necessary to perform the security break, the amount of time and money spent by the attackers.

One method of securing images is to encrypt image data using DES (Data Encryption Standard). However, DES is very complicated and involves large computations. A software DES implementation is not fast enough to process the vast amount of data
generated by multimedia applications, and hardware DES implementation adds extra cost on both broadcasters and receivers.

Due to special property of compressed image structure, and through selective encryption of parts of the bit-stream, the processing time can be highly reduced while a reasonable level of security is maintained. For this purpose, the bit stream data is classified into independent and dependent data. Hence, securing the independent data only would automatically insure the security of the dependent data.

This thesis had covered in brief the compression technique that are applied on images Chapter 2, the Bitmap and JPEG file format structure are addressed in Chapter 3, and the AVI and MPEG stream format are covered in Chapter 4. While Chapter 5 illustrated some of the commonly used encryption algorithms. Chapters 6 & 7 will be covering the simulation algorithms and results that were applied on selected images. And finally the Conclusion and results of the thesis was described in Chapter 8.