© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 29 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Encryption using SCAN Pattern & Image Encryption then Compression

[1]Rohit, Research Scholar, Department of ECE, CBS group of institutions, Jhajjar, India
[2]Chinar, Department of ECE, CBS group of institutions, Jhajjar, India

Abstract—Encryption Then Compression (ETC) system that ensures security and give compression ratios similar to the state of the art Compression then Encryption (CTE) systems has been an area of research recently. The existing Encryption Then Compression system encrypts using Prediction Error Clustering and Random Permutation and compress using adaptive arithmetic coding. The existing system gives only slightly worse compression ratio than CTE system. The need of sending cluster information makes it vulnerable to attacks. Statistical attack is also possible since it uses adaptive arithmetic coding for compression. The proposed system tries to overcome the shortcomings of the existing system by using hybrid approach for image encryption using SCAN patterns and carrier images at multiple stages and use adaptive arithmetic coding for compression.

Keywords— *Carrier Images; Compression of Encrypted image; Encryption Then Compression;Image Security; Prediction Error Clustering; Random Permutation; Scan Patterns*

I. INTRODUCTION

For sending an image securely to Bob, she can either use Compression Then Encryption (CTE) or Encryption Then Compression (ETC) system [1].

A. *Compression Then Encryption System*

A CTE system can be used if Alice is ready to pay the computational costs and has enough resources for doing so and Charlie is either lazy or resource deprived.

In a CTE system, Alice compresses the original image and then encrypts it and sends it to Charlie for forwarding it to Bob as depicted in Fig.1. Bob on receiving the image decompresses and then decrypts back.

First compressing then encrypting makes it less prone to brute force attacks, thus making it highly efficient system. As the encryption makes an image less correlated and thus less compressible, compressing an original image is a lot easier than compressing an encrypted image.

B. *Encryption Then Compression System*

Alice wants to send an image securely to Bob through a less trusted channel provider Charlie, but she is using a resource deprived device such as a mobile. So she is ready to encrypt it but can‟t afford cost for compressing the image.

© iJRPS International Journal for Research Publication & Seminar

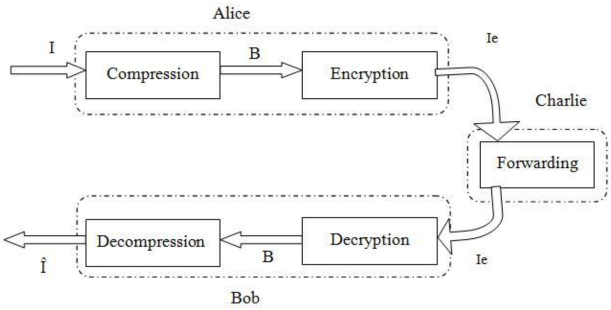

Fig.1. CTE System

Charlie has enough resources to compress the image. We make use of Encryption Then Compression system in such a scenario.

In an ETC, Alice encrypts the image and sends it to Charlie as depicted in Fig.2. Charlie does the compression and forwards the compressed image to Bob who decompresses and decrypts it to get back a reconstructed image.

Although encryption efficiency is good when compared to CTE system, many ETC systems designed so far is poor in compression. But the ETC system designed using prediction error clustering and random permutation is showing better compression efficiency than any existing CTE systems.

II. RELATED WORKS

In recent years Researchers were focusing on how to process encrypted signals in encrypted domain [3]-[7]. Although our existing compression algorithms are well suited for the unencrypted domain, Johnson et. al showed both theoretically and practically that we can compress the encrypted binary images.

Schonenberget. al later gave the idea of 1D and 2D source model based on LDPC codes [9], [10]. Lazzeretti and Barni investigated the possibility of compressing grey level and color images by using the idea of LDPC codes in various bit planes [11].