International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

# Analysis of Image Compression & Encryption Techniques

SALIGANTI UMAMAHESH,
Embedded System Trainer, Somarouthu Technologies, Hyderabad, Telangana, India

***Abstract**: The continuous growth of mobile, desktop and wired and wireless digital communication technologies has made the extensive use of the images unavoidable. The basic characteristics of image like transmission rate, bandwidth, redundancy, bulk capacity and co-relation among pixels makes basic compression algorithms mandatory. The research exploration in the field of image compression is huge. In this research paper we investigate the performance evolution of basic compression algorithms and encryption techniques on image data. We are adopting RLE (Lossless) compression and its modified version of algorithm, named K-RLE (Lossy) and AES (block cipher) for encryption. The basic and proposed system architecture, design, complexity, and performance could be analyzed and compare using MATLAB & VHDL Language, which is the quick tool to estimate performance of the system.*

**Keywords:** KRLE, image compression, lossy, Lossless, AES Encryption Technique, VHDL, MATLAB

## 1. INTRODUCTION

The rapid growth of multimedia and networking technologies gives rise to numerous multimedia applications such as mobile, desktop, internet and video surveillance, satellite communication and webcams, consequently multimedia transmission has become a challenge issue. Due to the unique characteristics of real time image data such as large data size, high bandwidth and stringent real time requirements. The researchers have been forcing to use the proper image compression algorithm to enhance the overall performance (compression ratio, saving percentage, compression time, entropy and code efficiency) of the system should be selected carefully for real time image transmission. Image compression is specialized discipline of electronic engineering as been gaining considerable

attention on account of its applicability to various fields. Image compression is art of representing information in compact form rather than it's original. Using the image data compression method, the size of particular image file can be reduced. Compressed image transmission economizes bandwidth, computation and transmission--power, cost, and latency and therefore ensures cost-effectiveness during transmission. the application areas for such compression today range from mobile, TV and broadcasting of HD-TV up to very high quality applications such as professional digital video recording or digital cinema / large screen digital imagery and so on this as lead to enhanced interest in developing tools an algorithms for very low bit rate image coding and image quality [2].

### 1.1 IMAGE

An image is essentially a 2-D signal processed by the human visual system. The signals representing images are usually in analog form. However, for processing, storage and transmission by computer applications, they are converted from analog to digital form. A digital image is basically a 2- Dimensional array of pixels. Each pixel has intensity value and location address. Images form the significant part of data, particularly in remote sensing, biomedical and video conferencing applications.

### 1.2 IMAGE COMPRESSION

The purpose of compression is to code the image data into a compact form, minimizing both the number of bits in the representation, and the distortion caused by the compression .the importance of image compression is emphasized by the huge amount of data in raster images, a typical gray-scale image of 512 x 512 pixels, each represented by 8bits, contains 256 kilobytes of data. With the color information, the number of bytes is tripled. The video images of 25 frames per second, even a one second color film requires approximately 19 Megabytes of Memory. To handle and process the above said data representation definitely one has to think of how to represent in terms of the encoded data the method is called compression, obliviously this technique becomes mandatory for any kind of present day digital image data processing

### 2.1 Related Work:

Till now many scientists, research scholars, Engineers proposed many data compression algorithms that compress almost any kind of data, In that the best know are the family of ZIV-Lempel algorithms. If the method is lossless they retain all the information of the compressed data, they doesn't take advantage of the 2-D nature of the image data. Only small portion of the data space can be saved by a lossless compression method. now a day's lossy techniques are widely used in image compression, because they produce high compression ratio and saving ratio, of course there may be image quality degradation when reproduction of original image from compressed image, however the image quality could be improved by selecting the appropriate compression technique / algorithm based on the application requirements In lossy compression, always there would be tradeoff between the bit rate and the image quality.

A common characteristic of most images is that the neighboring pixels are correlated and therefore contain redundant information. Two fundamental components of compression are redundancy and irrelevancy. Redundancy reduction aims at removing duplication from signal source. Irrelevancy reduction omits parts of the signal that will not be noticed by the signal receiver. There are three types of redundancies, they are spatial redundancy means correlation among neighboring pixel values, and coding redundancy is used when less than optimal code words are used, spectral redundancy means correlation between color planes and temporal redundancy means correlation between adjacent frames. Image compression techniques reduce the number of bits required to represent an image by taking advantage of these redundancies. An inverse process called decompression is applied to the compressed image data to get the reconstructed image. The two main distinct structural blocks of typical image processing system are an ***encoder*** and a ***decoder*** as shown in figure 1. Image f(x,y) is fed into the encoder, which creates a set of symbols form the input data and uses them to represent the image. If we let n1 and n2 denote the number of information carrying units( usually bits ) in the original and encoded images respectively, the compression that is achieved can be

quantified numerically via the compression ratio.

$$C_R = n1 / n2 \text{ ---------- } 2.1$$

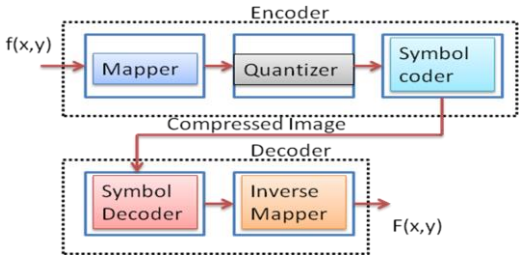


Figure 1

As shown in the figure 1, the encoder is responsible for reducing the coding, interpixel and psychovisual redundancies of input image. In first stage, the mapper transforms the input image into a format designed to reduce interpixel redundancies. The second stage, quantizer block reduces the accuracy of mapper's output in accordance with a predefined criterion. In third and final stage, a symbol decoder creates a code for quantizer output and maps the output in accordance with the code. These blocks perform, in reverse order, the inverse operations of the encoder's symbol coder and mapper block. As quantization is irreversible, an inverse quantization is not included in the figure 1.

The typical parameters, which are used to measure performance of the lossy image compression techniques / algorithms.

**Compression Ratio** is the ratio between the size of the compressed file and the size of the source file.

**Compression Factor** is the inverse of the compression ratio. That is the ratio between the size of the source file and the size of the compressed file.

**Saving Percentage** calculates the shrinkage of the source file as a percentage.

SP = (size before compression – size after compression) / size before compression

**Compression Time**

Time taken for the compression and decompression should be considered separately. Some applications like transferring compressed video data, the decompression time is more important, while some other applications both compression and decompression time are equally important. If the compression and decompression times of an algorithm are less or in an acceptable level it implies that the algorithm is acceptable with respective to the time factor. With the development of

high speed computer accessories this factor may give very small values and those may depend on the performance of computers or machines.

**ENCRYPTION PROCESS:**

The selective application of technological and related procedural safe guards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. This project specifies a cryptographic algorithm, the Advanced Encryption Standard (AES) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data.

Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the AES will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In this the key must be available at the transmitter and receiver simultaneously during communication.

In the existed design the security method uses Asymmetric Cryptography technique which provides different keys to sender and receiver to transfer the information. The transferred information is stored in the memory unit for further using it or for further processing using EEPROM and RAM. An AMBA bus is used to provide communication between the connected devices. A microcontroller is used to provide the patters for transmission through crypto unit.

In the proposed design the security method uses symmetric Cryptography technique which provides same keys to sender and receiver to transfer the information for reducing the design complexity. The transferred information is

stored in the memory unit for further using it or for further processing using low cost buffer element. A transmission cable is used to provide communication between the connected devices. Control logic is used to provide the patters for transmission through crypto unit.

## 3.0 IMAGE COMPRESSION TECHNIQUES

The image compression techniques are broadly classified into two categories, they are: Lossless techniques and Lossy techniques. In our research work we consider one lossy compression (K-RLE) and one lossless compression algorithms (RLE) on a standard Leena image data file (512x512x8).we evaluate the performance of these algorithms by calculating or measuring the typical parameters discussed in the above section.

### 3.1 LOSSLESS COMPRESSION TECHNIQUE

In lossless compression techniques, the original image/data can be perfectly recovered from the compressed (encoded) image/data. These are also called noiseless since they do not add noise to the signal (image).It is also known as entropy coding since it use statistics or decomposition techniques to eliminate or minimize redundancy. Lossless compression is used only for a few applications with stringent requirements such as medical imaging and sensor data processing, ***In our research work we consider the basic lossless compression technique named as Run Length Encoding (RLE),*** earlier researchers implemented the RLE compression algorithm on low cost, low power tinny embedded systems (based on 8bit/16bit microcontrollers) using ALP and respective EC programming for slowly varying sensor data for wired and wireless sensor networks (WSN) [4]. Even they evaluated the performance of RLE on Reconfigurable FPGA Architecture for above said applications [5]. Probably no one analyzed design exploration of image data compression using RLE. In our research work we analyze and evaluate the performance of RLE compression algorithm for image data applications based on MATLAB EDA Tools

#### 3.1.1 Run – Length Encoding:

- The Idea behind this algorithm is, If a data item d occurs n consecutive times in the input data we replace the n occurrences with the single pair nd.
- Run-Length Encoding (RLE) is a basic compression algorithm. It is very useful in case of repetitive and slowly varying data items.
- This is most useful basic compression algorithm on data that contains many such runs: for example, relatively simple graphic images such as icons, line drawings, and grayscale images.
- Which is a lossless data compression algorithm used for slowly varying sensor and image data.
- It is not useful with files that don't have many runs as it could double the file size.

### 3.1.2 Flow Chart for Run Length Encoding:

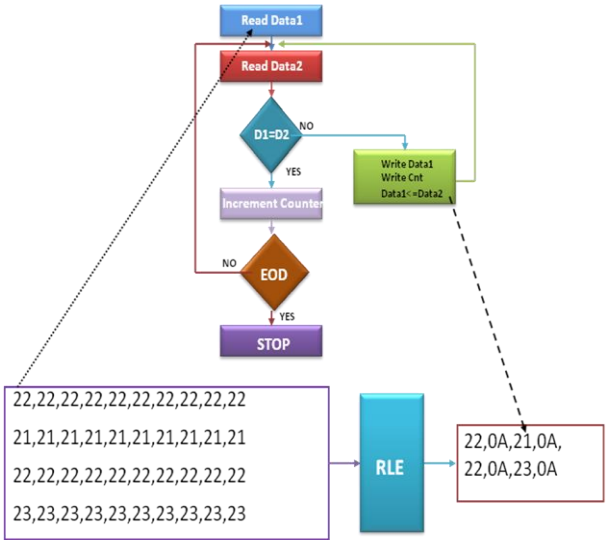


**Figure 2**

### 3.2 LOSSY COMPRESSION TECHNIQUE

Lossy schemes provide much higher compression ratios than lossless schemes. Lossy schemes are widely used since the quality of the reconstructed images is adequate for most applications .By this scheme, the decompressed image is not identical to the original image, but reasonably close to it.

### 3.2.1 Run Length Encoding with K - Precision:

The idea behind this new proposed algorithm is this: let K be a number, a data item d or data between d+K and d-K occur n consecutive times in the input stream,

replace the n occurrences with the single pair nd. We introduce a parameter K which is a precision.

- If K = 0, K-RLE is RLE. K has the same unit as the dataset values, in this case degree.
- K-RLE is a lossy compression algorithm.
- This algorithm is lossless at the user level because it chooses K considering that there is no difference between the data item d, d+K or d-K according to the application.

### 3.2.2 Flow Chart for Run Length Encoding with K - Precision:

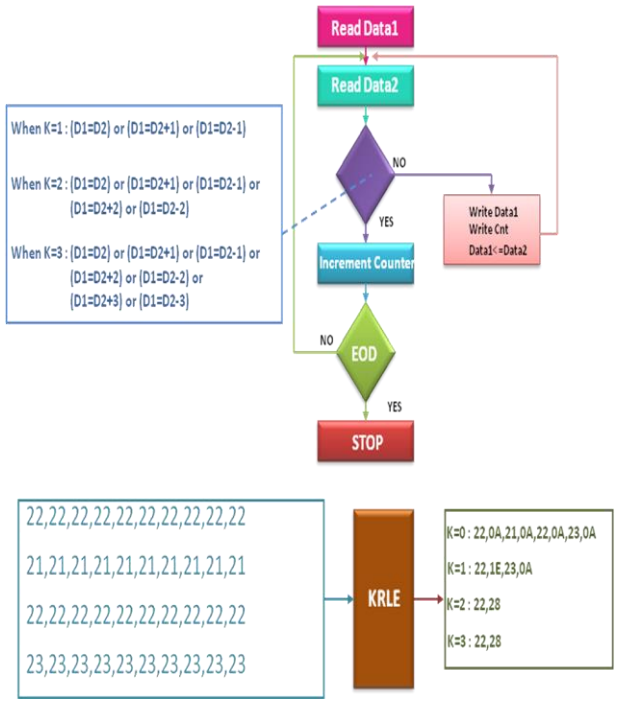


**Figure 3**

## REFERENCES:

[1] jayavrinda vrindavanam, saravanan chandran and gautam k.mahanti, 2012, A survey of image compression methods, IJCA.

[2] S.R Koditvwakku and u.s. amarasinghe , comprasion of lossless data compression algorithms for text data, IJCSE, vol 1 no 4 410 – 425.

[3] B.subramanyan, vivek.m.chhabria and T.G sankar babu, 2011, image encryption based on aes key expansion, IEEE

[4] eugene pamba cupo – chichi, herve guyennet and jean – michel friedt, 2009, KRLE – A new data compression algorithm for wireless sensor network, IEEE

[5] Wail s.elkilani, hatem m.abdul – kadar, 2009, performance of encryption techniques for real time video streaming, IEEE

[6] K.Arshak, E.jafer, D.mcdonagh and c.s.ibala, 2007, modelling and simulation of wireless sensor system for health monitoring using HDL and simulink mixed enviroment, IET computer. digital tech vol 1. No 5, September.

**PROFILE:**

I, Saliganti Umamahesh completed my PG in the stream of VLSI & Embedded System. Currently working as embedded system trainer in Somarouthu Technologies, Hyderabad.