Image Compression with Partial Encryption using Hill Cipher

AmishaMadhwani, PranaliDeogade, PriyankaManwatkar
Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur.

Abstract-Existing techniques when utilize compression there is no thought of security, correspondingly when it portray encryption there is no thought of size i.e. compression. There are two methodologies CE i.e. compression took after encryption and EC i.e. encryption took after compression. In our task, our succession will be EC i.e. image encryption is performed first then the image compression is connected. For image encryption we will utilize slope figure. Correspondingly for compression we will utilize Discrete Cosine Transform. In the proposed approach, we are not utilizing CE in light of the fact that an interloper has less intimation to get to image yet encryption might again build the size. To spare the transfer speed fractional encryption is done in light of the fact that image transmission is required two times. Firstly, when quarter image is send and furthermore when entire packed image is send.

Keywords: Key, Image Compression, Image Encryption.

I. INTRODUCTION

We are managing huge measure of information in the field of image preparing. Image compression calculations use to diminish the measure of information required to speak to an advanced picture and the premise of the decrease procedure is the evacuation of spatial and psycho visual redundancies. Scientifically, information compression ordinarily includes changing (encoding) a 2-D pixel cluster into a measurably uncorrelated information set. Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that producible differences may be called visually lossless. Two sorts of compression are lossless compression and lossy compression. In the event that same image can be produced from the packed image then it is Lossless compression else it is Lossy compression. However alone compression is not adequate as it has an open access, anyone can get to it. So on the off chance that it is fancied that it can be available just by approved individual it ought to be scrambled too. The encryption can be performed either using so as to utilize Symmetric key cryptography or Asymmetric key cryptography. On the off chance that same key is utilized for encryption and decoding then it is called as symmetric key cryptography and if the diverse key is utilized for encryption and decoding then it is called as asymmetric key cryptography. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption and decryption should not be confused with encoding and decoding, in which data is converted from one form to another but is not deliberately altered so as to conceal its content.

II. PROBLEM DEFINITION

An Approach to image compression, with fractional Encryption without sharing secret key. Aimage of gray scale is isolated into four equivalent amounts of size. One quarter part is encoded and after that consolidate with remaining part. This image is packed and sends to recipient. Beneficiary decodes it by utilizing its own particular private key. We are doing this with a specific end goal to accomplish secure image exchange in the middle of sender and beneficiary by decreasing data transfer capacity.
III. LITERATURE SURVEY

The literature work can be categorized with respect to the application of the two processes image compression and image encryption as:

a) Compression followed by Encryption (CE)
In this sequence an intruder has fewer clues to access the image but encryption may again increase the size.

b) Encryption followed by Compression (EC)
In this sequence size is not again increased but the intruder may have more clues to access the image.

c) Joint Compression and Encryption (JCE)
This approach is in use these days, which may be fast as compared to previous two but procedure is complicated.

In this area, an investigation of different examination papers in view of picture encryption/unscrewing and pressure methods and execution parameters which can assume an imperative part to enhance the productivity and security of calculation is exhibited. In [1] creator presents a novel investigation of three square figure (RC6, MRC6, and Rijndael) calculations. In this paper creators have scrambled distinctive sorts of Bitmap pictures with each of the above three encryption calculations and measured the most extreme deviation between the first and the encoded pictures, the connection coefficient between the encoded and the first pictures, the contrast between the pixel estimation of the first picture and its comparing pixel estimation of the scrambled one, the encryption time and the throughput. These variables were connected on the three encryption calculations to assess both: pictures containing numerous high recurrence segments and pictures containing substantial regions of single hues, as samples of parallel pictures.

In [2], creators have presented a piece construct change calculation situated in light of the mix of picture change joined with an understood encryption and decoding calculation, Blowfish. Here the first picture was partitioned into pieces which were revamped into a changed picture utilizing the aforementioned change calculation and after that the changed picture was encoded utilizing the Blowfish calculation. The outcomes demonstrated that the connection between picture components was essentially diminished by utilizing this procedure. The outcomes additionally demonstrate that using so as to expand the quantity of squares little piece sizes brought about a lower connection and higher entropy.

In [3], creators have displayed reproduction results taking into account the parameters like visual testing, key space examination, histogram investigation, data entropy, encryption quality, connection investigation, differential examination, affectability examination and execution examination. Salsa20, the strategy utilized as a part of the paper for ensuring the appropriation of advanced pictures in a proficient and secures way.

In [4] creator presents paper when the data capacity/waveform is intermittent, the Fourier change yield is a Dirac brush capacity, balanced by a discrete succession of limited esteemed coefficients that are mind boggling esteemed by and large. These are called Fourier arrangement coefficients. The term Fourier arrangement really alludes to the converse Fourier change, which is a whole of sinusoidal at discrete frequencies, weighted by the Fourier arrangement coefficients. When the non-zero part of the information capacity has limited span, the Fourier change is persistent and limited esteemed. In any case, a discrete subset of its qualities is adequate to remake/speak to the bit that was investigated. The same discrete set is acquired by treating the term of the portion as one time of an occasional capacity and processing the Fourier arrangement coefficients.

In [5], creator has introduced a novel and hearty tumult based cryptosystem for secure transmitted pictures and four different forms. Here creator has proposed a piece encryption/unscrewing calculation where they have rearranged the picture pixel position by 2D turbulent guide, trailed by substitution (perplexity) and change (dispersion) operations on each square, with different rounds, joined utilizing two irritated disordered PWLCM maps. The irritating circle method enhances the measurable properties of scrambled pictures. The acquired mistake spread in different standard figure square modes shows that the writer's cryptosystem is suitable to transmit figure information over an undermined advanced channel. At long last, creator has attempted to demonstrate that his cryptosystem has a high security level on the premise of numerous tests.

IV. PROPOSED SYSTEM

In our proposed framework investigate some standard shading image is done. Secured image compression is performed by applying encryption took after by compression. The benefit of the proposed strategy is that the encryption and decoding of image is completed at sender and collector side without trading or sharing the secret key. Yet, image compression is required to spare the data transfer capacity halfway encryption is finished. For encryption any symmetric key cryptosystem can be utilized like AES, DES or multiplicative figure. Be that as it may, we are utilizing Hill Cipher calculation for encryption in our undertaking. The investigations are performed utilizing multiplicative figure. Thus for compression and decompression any lossless compression procedure can be utilized.

The block schematic of the proposed scheme is shown in Fig. 1.
Fig. 1 Block Schematic of the proposed Approach

V. HILL CHIPER ALGORITHM

The Hill cipher is an example of a block cipher. A block cipher is a cipher in which groups of letters are enciphered together in equal length blocks. The Hill cipher was developed by Lester Hill and introduced in an article published in 1929.

**Example:**

**Encrypt**

In order to encrypt a message using the Hill cipher, the sender and receiver must first agree upon a key matrix $A$ of size $n \times n$. $A$ must be invertible mod 26. The plaintext will then be enciphered in blocks of size $n$. In the following example $A$ is a $3 \times 3$ matrix and the message will be enciphered in blocks of 3 characters.

$$
A = \begin{bmatrix}
17 & 17 & 5 \\
21 & 18 & 21 \\
2 & 2 & 19
\end{bmatrix}
$$

Key Matrix: $A =$

Plain Text: PAY MORE MONEY

Block of character: PAY MOR EMO NEY

The first block plain text corresponds to the matrix

$$
\begin{bmatrix}
15 \\
0 \\
24
\end{bmatrix}
$$

The sender will then calculate:

$$
C = \begin{bmatrix}
17 & 17 & 5 \\
21 & 18 & 21 \\
2 & 2 & 19
\end{bmatrix}
\begin{bmatrix}
15 \\
0 \\
24
\end{bmatrix} \mod 26
$$

$$
C = \begin{bmatrix}
11 \\
13 \\
18
\end{bmatrix}
$$

The first three letters of the cipher text correspond to 11, 13, 18 and are therefore LNS. This step is repeated for the entire plaintext. If there are not enough letters to form blocks of 3, pad the message with some letter, say X.

The message: PAY MOR MON ENY

Will be enciphered as:

LNS HDL EWM TRW

Notice that the repeated digraphs IS, SS and repeated letters S and P in the plaintext are masked using the Hill cipher.

**Decipher**

To decipher a message, first calculate the inverse of the key $A$.

Then multiply the inverse of the key by each pair of cipher text letters (mod 26) to recover the original text.

Key Matrix:

$$
A^{-1} = \begin{bmatrix}
4 & 9 & 15 \\
15 & 17 & 6 \\
24 & 0 & 17
\end{bmatrix}
$$

Encrypted Message: LNSHDLEWMTRW

The receiver will calculate:

$$
\begin{bmatrix}
11 \\
13 \\
18
\end{bmatrix}
\begin{bmatrix}
4 & 9 & 15 \\
15 & 17 & 6 \\
24 & 0 & 17
\end{bmatrix} \mod 26 = \begin{bmatrix}
15 \\
0 \\
24
\end{bmatrix}
$$

To decrypt the message, the first three letters are 15, 0, 24 which correspond to PAY. The receiver will repeat this step for every pair of letters in the cipher text to recover the original message PAYMORMONEY.
To use a Hill cipher with different block size the number of rows and columns in matrix $A$ should be equal to the block size. For example if the block size is 4 the $A$ should be a matrix of size $4 \times 4$.

VI. DETAILS OF COMPLETED MODULES WITH SUPPORTING RESULT

Till now in our project we have completed the sender part as shown in the block diagram. Supporting result of our project is shown in screenshots which are as follows:

- Fig.2 Front Screen
  In fig. 2 we have shown the front screen of our project. From the open option as shown in ribbon interface we select the image which we want to perform encryption and compression transformation.

- Fig.3 Conversion of image to gray scale
  In fig. 3 we have shown the conversion of image from RGB image to grayscale image since we have to map each bit of image for encryption. In RGB images no of bits values are more since we have all values of RGB while in grayscale we need to consider only B values Rand G values are zero here.

- Fig.4 Division of image into four parts
  In fig.4 we have divide the image into 4 parts using simple division algorithm.

- Fig.5 Encryption of 1 part
  In fig.5 we have perform encryption for the one part using Hill Cipher algorithm.

CONCLUSION

In this paper, a large portion of the current vital image compression and encryption strategies have been exhibited and investigated. The most ideal method for quick and secure transmission is by utilizing compression and encryption of media information like images. The exploration works have been arranged in the accompanying three classifications in view of the request of the two procedure viz., CE, EC or JCE. Encryption connected by various scientists by method for encoding calculation which scramble the whole or incomplete media bit arrangement utilizing a quick routine cryptosystem. A significant part of the past and flow research targets scrambling just a deliberately chose part of the image bit stream so as to lessen the computational load, and yet keep the security level high. In this manner for accomplishing both components like security and low data transfer capacity transmission we utilized both encryption and pressure procedures and we have accomplish these both variables in our task.
REFERENCES


