Research Paper Education

Genetic Image Compression & Encryption

Syed Mahamud Hossein

Regional Office, Directorate of Vocational Education and Training, West Bengal, Kolaghat-721154,Purba Medinipur, India

ABSTRACT

This proposed encryptions and lossless compression technique designed for large genetic image. The basic try-compression scheme presented is based on a modified Huffman techniques & selective encryption which enables fast encryption of a large amount of digital data. Also assess its performances in terms of processing time, compression ratio, rate and selective Encryption technique. The compression reduces file size & encryption ensures the security of a particular file which is to be sent over some unreliable network like internet. Security on image is the serious issue now-a- days. At first, digitized a image file using MATLAB, produced text file. In Joint encryption process, first; use modified Huffman algorithm for compression as well as selective encryption and in secondly use selective encryption techniques for better securities.

KEYWORDS Image, Compression, Security, selective encryption and Huffman's

INTRODUCTION

Image compression is used to minimize the amount of memory needed to represent an image. Image often require a large number of bits to represent them and if the image needs to be transmitted or stored, it is impractical to do so without somehow reducing the number of bits. The problem of transmitting or storing an image affects all of us daily. The objective is to reduce redundancy of the image data in order to be able to store or transmit data in an efficient form. Joint compression and encryption have been extensively studied over the past decade [1-3].

Directly applying standard encryption techniques, such as DES and AES[4],becomes prohibitive due to the processing time. Selective encryption where a part of a whole message encrypted, keeping the other remain as it is in such a way that the security is not compromised[5]. This technique test on data used in [6].

This selective encryption approach not only reduces the time complexity for encryption and decryption due to encryption of only the part of the compressed data where reconstruction information are mostly concentrated and but also it reduces the storage and communication cost.

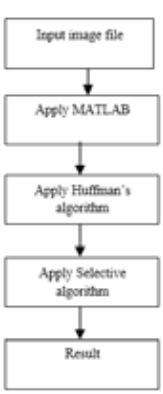


Figure-1

Its features are as follows: (1) low computational complexity, (2) high security, and (3) no distortion. On the other hand, confidentiality and access control are addressed by encryption through which only authorized parties having the decryption key can be access the encrypted content[7-8]. Speed of encryption and security levels are two important measurements for evaluating any encryption system.

GENERAL APPROACH

CONVERSION of IMAGE to PIXEL-MATRIX:

We have written a MATLAB program for conversion image to digitization.

CODE:

```
A=imread ('a.jpg')
imshow (A)
I=rgb2gray (A)
B=double (I)
dlmwrite ('Proj.txt',B,' ')
```

For Try-Compression System Two Separate Modified Huffman Algorithm Scheme Are Use :

Here used the Huffman's Compression Algorithm which reads a text file (*.txt).The text-file can contain numbers, text, ASCII characters or combination of them. For that purpose, need to generate the Pixel- Matrix of the image (to be compressed) and write it onto a text-file. The Compression program would then read this text-file as input and generate the corresponding compressed & encrypted file, by selective encryption algorithm and ultimately getting the result.

This algorithm recursively find a weighted binary tree with n given weights w_1, w_2, ….w_n. (Here weights mean frequency of n characters in text). LEVEL is the input where the tree is altered.

I) Swapping Nodes At Specified Level (Scheme-I)

Here swapping of the branches in the Huffman tree on at a particular level on the basis of a key and decode the encoded symbols using the modified Huffman tree. Here, exchange left most node with right most node at specified level. So only those nodes, which are changed their positions after swapping, are affects and also corresponding codes are also altered.

Algorithm for Scheme-I:

- Arrange the weights in increasing weights.
- Construct two leaf vertices with minimum weights, say w_i and w_j in the given weight sequence and parent vertex of weight $w_i + w_j$.
- Rearrange remaining weights (excluding w_i and w_j but including parent vertex of weight $w_i + w_j$) in increasing order.
- Repeat step 2 until no weight remains.
- Find out left most node and right most node at specified LEVEL and interchange their position with respect to their parent node.
- To find out code for each given weights (i.e. frequency of

characters) traversing tree from root assign when traverse left of each node & 1 when traverse right of each node.

II)Swapping Between Two Specified Nodes At Different Level (Scheme-Ii)

In this scheme, need to specify two level values of two nodes and two binary values. Number of binary digit must be same with level value with respect to nodes. If consider above specified two values as a key then security concern is improved than before experiment.

Algorithm for scheme-II:

- Arrange the weights in increasing weights.
- Construct two leaf vertices with minimum weights, say w_i and w_j in the given weight sequence and parent vertex of weight $w_i + w_j$.
- Rearrange remaining weights (excluding w_i and w_j but including parent vertex of weight $w_i + w_j$) in increasing order.
- Repeat step 2 until no weight remains.
- Find out two nodes at specified LEVEL by binary digits and interchange their position with respect to their parent node.
- To find out code for each given weights (i.e. frequency of characters) traversing tree from root assign when traverse left of each node & 1 when traverse right of each node.

III) Applying Selective Compression On Compressed Data (Scheme-III)

Selective encryption are apply in three ways i) Select only single character ii) select Numeric numbers only iii) Pattern selection . Also generate private and public key.

Algorithm for scheme-III:

Selective Encryption Algorithm

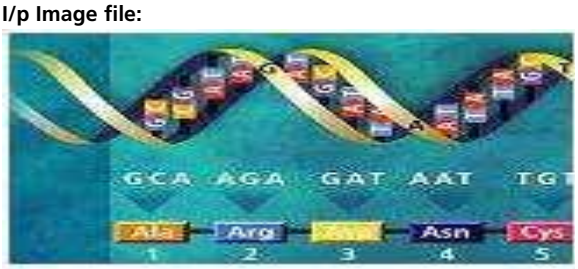
- Input File Name with Path.
- Select Number or a Specific String.
- Use RSA algorithm for encryption of the selected Number or Specified String.
- Generate an Auxiliary File to keep the Flag for the specific regions of the Encrypted data.
- Generate the Encrypted Output file.
- Generate the Public Key and Private Key ultimately.

Selective Decryption Algorithm

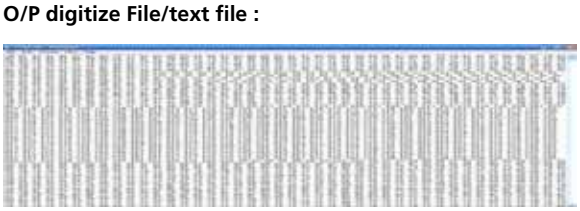
- Open Encrypted and Auxiliary File.
- Input Encryption Option.
- Read Encrypted data from Auxiliary File.
- Use Private key to Decrypt data using RSA Module.
- Get the Decrypted Output file.

RESULTS

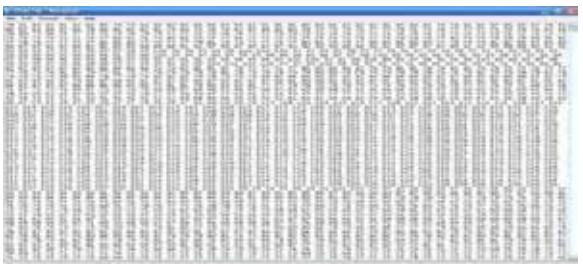
I/p Image file:



O/P digitize File/text file :



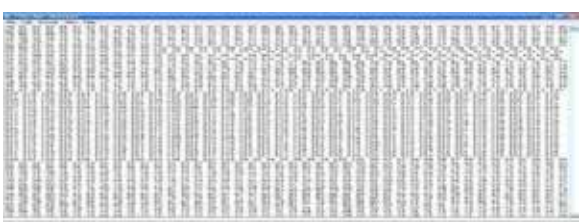
Compression by Huffman Algorithm:



Apply encryption algorithm

Decompression by Huffman & Decryption Algorithm

O/P FILE:

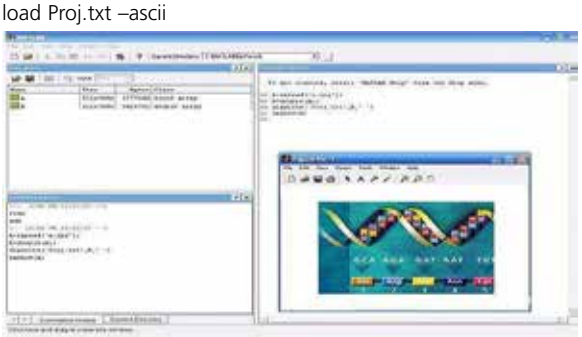


RESTORING the IMAGE:

The decompressed text-file obtained as an output from the decompression program, has to be loaded into the MATLAB workspace to restore the image and image should have the exact same properties(intensity, colour, hue, quality etc) as that of the original image The decompressed text file has to be manually copied into the 'Work' folder of MATLAB.

CODE:

load Proj.txt –ascii



I=mat2gray(Proj) Imshow(I)

DISCUSSION

The encrypted compressed file then can be decrypted & decompressed at the client end resulting in reduced transmission time over the Internet. A encrypted compression algorithm that provides a moderately high compression with encryption rate with minimal decryption with decompression time. The running time of this algorithm is very few second, varies linearly with the size of the source file to be compressed.

The input image size is 404kb, after compression the size is reduce to 195kb. Also observed that no change in file size, if apply selective encryption algorithm.

CONCLUSION:

Here used three different schemes; in scheme-I swapping of

nodes is done at specified level based on key, in scheme-II swapping is done between two specified nodes at different levels and scheme –III using selective encryption method. This experiment found that the effectiveness of the encryption system increases as the level at which swapping is done & increases.

Also if consider word instead of characters then workspace is increased. So the probability of frequency analysis attack is low.

In case of character encryption, here only 256 characters are available and since workspace is short. So here is a possibility to break the security. But in case of word encryption, numbers of distinguishable words are huge, not known by all, so that workspace is so increased and breaking the security is not possible.

ACKNOWLEDGEMENTS
Above all, author are grateful to all our colleagues & friends of A.Mitra and S.Roy, Haldia Institute of Technology, Haldia or their valuable suggestion, moral support, interest and constructive criticism of this study. The author offer special thanks to Ph.D guides for helping in carrying out the research work also like to thank our PCs.

REFERENCES

[1]X.Liu and A.M.Eskicioglu, "Selective encryption of multimedia content in distribution network: Challenges and new directions," in Int. Conf. on Communication, Internet, and Information Technology,2003, pp527-533 | | [2] S.S. Maniccam and N.G.Bourbakis,"Lossless image compression and encryption using scan," in pattern recognition,2001, vol.34,pp.1229-1245 | | [3] H.Cheng and xiaobo Li, " Partial encryption of Compressed images and videos," in IEEE Trans. Signal processing,2000, vol.48,pp.2439-2451 | [4] J.Daemen and V. rijmen, "AES proposal, rijdael," in The First Advanced Encryption Standard candidate Conference, N.I.S.T.,1998 | | [5] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Video," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451. | [6] Free available from website | [7] W.Diffie amd M.E.Hellman," New Directions in Cryptography," IEEE Transaction of Information Theory,vol.22, no. 6,pp.664-654, November 1976. | [8] W.Stalling, Cryptography and Network Security. Englewood Cliffs, New Jersey: Prentice Hall,2003