INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

HIDING DATA IN A COMPRESSED IMAGE USING MODIFIED HAAR COMPRESSION TECHNIQUE

Dr. Saad Abdual Azize
saadabdualazize@yahoo.com
Al mamoon University collage, Iraq, Baghdad

Abstract: - In the fields of communication and security, cryptography and compression became related and most important. Compressed files could have hidden data to be transmitted along the channels without been noticed. In this research, encrypted message is hidden, using new encrypting and hiding method, within an image which is compressed using modified Haar technique.

Key words: cryptography, hiding technique, Haar compression.

1- Introduction

Data compression is a method used in the beginning for saving storage area, and then it became an initial process in data communication in which data is compressed before it is sent in communication channels. Two essential types of compression are: lossless and lossy compression. Lossless compression is the type in which data after decompression is kept the same as before compression, which means, the original data is retrieved as a whole [1]. Compression is an important aspect in real time and online communication where transmission time is very important. Many different types of methods were used for compressing data; Haar wavelet compression is one of the efficient ways used to perform lossless and lossy compression. It depends on finding the average and the difference values for image pixels (matrix) and produce anew matrix which is sparse or nearly sparse [2]. A sparse matrix is the matrix where most of its elements are 0. A sparse matrix then will be stored in an efficient way making the file size much smaller.

To transmit a message secretly, hiding techniques should be used to embed the secrete massage within a covered media (image, audio, video) [3]. To hide a text message within a covered image, a new technique is proposed here where the only predefined parameter, that has to be identified, is the starting pixel only and the rest will be found with simple but yet unpredictable calculations.

The proposed method suggested that the spare matrix used in compression is created depending on the cover image pixels instead of using the original Haar matrices. This gives more plasticity and efficiency for the compression. The research also proposed a new method for encrypting and hiding the data in the image by using the values of data itself as indices for the positions where a message will be hidden. The proposed method transmits hidden messages secrecy and efficiently with variable keys which is practically important in on-line and real time systems.

2- Haar compression:

The process will be explained on 8x8 matrix. The process can be generalized to $2^k \times 2^k$ matrix, where k is a positive integer number. The corresponding matrix should be divided into 8x8 blocks and considering each block as a separate matrix. If there are 2^k elements in row of a matrix, then the row transformation process of matrix will consist of k steps. In our case k = 3, $(8=2^3)$ [4].

Below are the original Harr matrices:

$$W_1 = \begin{bmatrix} 1/2 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & -1/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 1/2 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & -1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 0 & -1/2 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & -1/2 \end{bmatrix}$$

$$W_2 = \begin{bmatrix} 1/2 & 0 & 1/2 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & -1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 1/2 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & -1/2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$W_3 = \begin{bmatrix} 1/2 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & -1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$W = W_1 W_2 W_3 = \begin{bmatrix} 1/8 & 1/8 & 1/4 & 0 & 1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & 1/4 & 0 & -1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & 1/2 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & -1/2 & 0 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & 1/2 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & -1/2 & 0 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & 1/2 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & -1/2 \end{bmatrix}$$

2-1 Haar Compression

To compress a data in matrix A, apply the compression equation (1) to get the compressed matrix S.

$$S = W^T A W \quad \ldots\ldots (1)$$

2-2 Haar Decompression

To decompress the matrix S, apply the decompression equation (2) to get the uncompressed data matrix A.

$$A = (W^T)^{-1} S W^{-1} \quad \ldots\ldots\ldots (2)$$

3- The Proposed Algorithm:

The process involves many operations each corresponding to a different part and algorithm. The whole process has two basic sides, sender and receiver, the sender has to encrypt the message, hide it in a cover image, compress the image then send it to the receiver how has to decompress the received image, extract the secret message and finally decrypt it.

3-1 Part one: Sender process

3-1-1 Phase 1: Message Encryption

1- Read the plain text (message)
2- Let the key (K) be the sequence of the characters in the plain text
3- Convert the characters to ASCII then subtract from 65
4- Encrypt the characters using Direct algorithm with key (K), call the result 'output'.
5- Find (M= 'output' mode 13)
6- If the 'output' is greater than 13 multiply M by 2 else multiply M by 2 then add 1.

3-1-2 Phase 2: Message Hiding

1- Identify the starting pixel in the covered image (should be secret).
2- Save in that pixel the first value of the encrypted message.
3- Add the value of the message to the x-axes value of the pixel's position to get the new location (new pixel were the data will be stored).
4- Save the second value of the encrypted message in the new pixel, then add the value to the y-axes to get the new next location.
5- Repeat the process of 3 and 4 till the entire message is saved.
6- In location (1,1) save the message length(number of hidden characters).

3-1-3 Phase 3: Compression using *Modified Haar*

1- Divide the image with hidden message into sub images A (8x 8).
2- For each sub image, find the *max* and *min* value.
3- Let L = min/max.
4- Create H (8x8) matrix which diagonal equals L (modified matrices).
5- Find the compressed matrix B(8x8), as in equation (3);

$$B = H A H^{-1} \quad \ldots\ldots\ldots (3)$$

6- Repeat for all sub images.

Now we get a compressed image, includes the hidden message, ready to be transmitted.

3-2 Part two: Receiver process

3-2-1 Phase 1: Decompression

Apply the same previous steps of phase 3 in reverse order except that the decompression (step 5) will be will apply equation (4);

$$A = H\ B\ H^T \text{ …….(4)}$$

3-2-2 Phase 2: Retrieve hidden Message

Apply the same previous steps of phase 2 in reverse order except that instead of saving data, read the data from pixels.

3-2-3 Phase 3: Decryption

1- Read the number of hidden characters from pixel(1,1).
2- Read the value (V) in the first pixel (starting pixel).
3- Find the value of R by equation (5);

$$R = V \text{ Div } 2 \text{ …….(5)}$$

4- If value (V) greater than 13 then use equation (6) to find Char;

$$Char = (R + 13 - key_i) + 65 \text{ ……(6)}$$

Else use equation (7) to find Char;

$$Char = (R - key_i) + 65 \text{ ……..(7)}$$

5- Find the next new location.
6- Repeat steps 1:5 till all the message is found.

4- Implementation

Let the plain text be:

Plain text = 'SECURITY'

Then:

KEY : 1 2 3 4 5 6 7 8

Message Characters : S E C U R I T Y

The whole process is shown in table (1) below:

Table 1: Implementation of sender process

Character	ASCII	Sub 65	Encryption Mod 26 (output)	Mod 13	Add 1 or 0
S	**83**	**18**	**19**	**6**	**13**
E	**69**	**4**	**6**	**6**	**12**
C	**67**	**2**	**5**	**5**	**10**
U	**85**	**20**	**24**	**11**	**23**
R	**82**	**17**	**22**	**9**	**19**
I	**73**	**8**	**14**	**1**	**3**
T	**84**	**19**	**0**	**0**	**0**
Y	**89**	**24**	**6**	**6**	**12**

Save (8) in pixel(1,1).

Suppose the start pixel is at location (2,1), Save 13 in that pixel.

The new location will be:

(2,1) + (13,0) = (15,1), save 12 in pixel(15,1).

The next new location will be:

(15,1) + (0,12) = (15,13), save 10 in pixel(15,13).

The next new location will be:

(15,13) + (10,0) = (25,13), save 23.

The next new location will be:

(25,13) + (0,23) = (25,36), save 19.

The next new location will be:

(25,36) + (19,0) = (44,36), save 3.

The next new location will be:

(44,36) + (3,0) = (47,36), save 0.

The last new location will be:

(47,36) + (0,0) = (47,36), save 12.

The proposed algorithm was applied on figure (1) below, to hide the message previously encrypted.

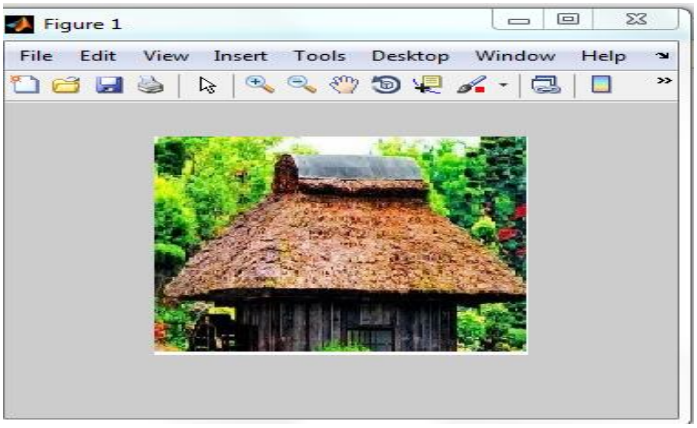

Figure 1: Original image

The image was splitted into the essential colors (red, green, and blue) to obtain the following three images in figure (2).

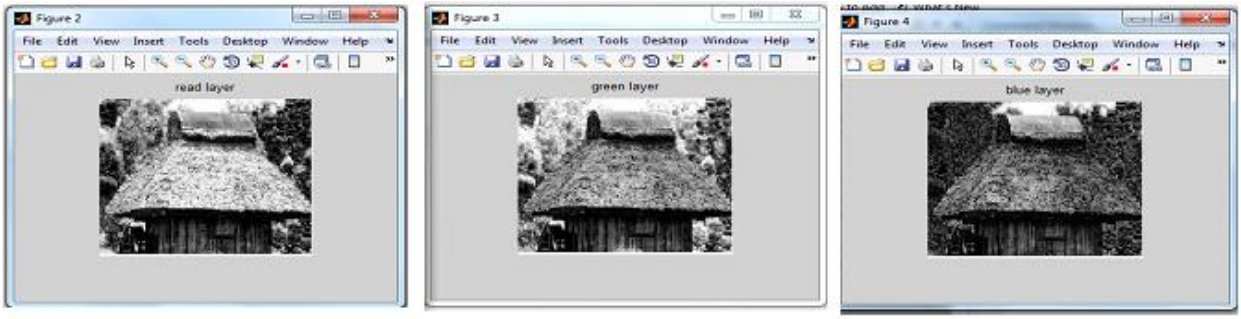

Figure 2: red, green and blue sub images

The secret message will be hidden in red part only (could be any part). Using one part of the colors make the effect of changes as minimum as possible. The image is then compressed and sends to a receiver who is going to decompress the received image, split it to get red part, extract the secret message, and then decrypt it to get the plan message.

5- Conclusion

The encryption algorithm uses the sequence of characters as a key to ensure that no two same characters will lead to same encryption value. The hiding technique depends on one secret value, the starting point. The other values will be extracted from the hidden data and the location. The modified compression method not only shrinks the size of the transmitted data but also makes the cryptanalysis of the hidden data impossible. All these combined techniques create a secure and efficient cryptosystem.

REFERENCES

[1] Data compression, David Salomon, 3rd edition, 2004.
[2] Introduction to data compression, Guy E. Blelloch, 2010.
[3] Cryptography and network security, William Stallings, 5th edition, 2011.
[4] IMAGE COMPRESSION USING THE HAAR WAVELET TRANSFORM , Mr. Hermina Alajbegović Dr. Dževad Zečić , Mr. Almir Huskanović , 13th International Research/Expert Conference ”Trends in the Development of Machinery and Associated Technology” TMT 2009.
[5] Computer security and cryptography, Alan G. Konheim, 2007.
[6] The Modified 2D-Haar Wavelet Transformation in Image Compression, P. Raviraj and M.Y. Sanavullah, Middle-East Journal of Scientific Research 2 (2): 73-78, 2007.