International Journal of Computer Applications Technology and Research
Volume 3– Issue 3, 136 - 139, 2014, ISSN: 2319–8656

Image Steganography Using HBC and RDH Technique

Hemalatha .M
Sri Manakula Vinayagar Engineering College
Pudhucherry, India

Prasanna.A
Sri Manakula Vinayagar Engineering College
Pudhucherry, India

Dinesh Kumar R
Sri Manakula Vinayagar Engineering College
Pudhucherry, India

Vinoth kumar D
Sri Manakula Vinayagar Engineering College
Pudhucherry, India

Abstract**:** There are algorithms in existence for hiding data within an image. The proposed scheme treats the image as a whole. Here Integer Cosine Transform (ICT) and Integer Wavelet Transform (IWT) is combined for converting signal to frequency. Hide Behind Corner (HBC) algorithm is used to place a key at corners of the image. All the corner keys are encrypted by generating Pseudo Random Numbers. The Secret keys are used for corner parts. Then the hidden image is transmitted. The receiver should be aware of the keys that are used at the corners while encrypting the image. Reverse Data Hiding (RDH) is used to get the original image and it proceeds once when all the corners are unlocked with proper secret keys. With these methods the performance of the stegnographic technique is improved in terms of PSNR value.

Keywords: ICT, IWT, HBC, RDH, Pseudo Random Number, Secret Key.

1. INTRODUCTION

One of the successful reasons behind the intruders to acquire the data easily is due to the reason that the system is in a form that they can read and comprehend the data. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography become more important as more people join the cyberspace revolution. Due to advances in ICT, most of information is kept electronically. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

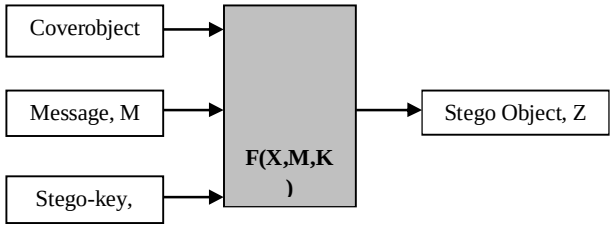

Figure 1: Encryption of an Image

There are many methods that can be used to detect Steganography such as: "Viewing the file and comparing it to another copy of the file found on the Internet (Picture file). The Proposed System consists of the different methods to be used in the encryption and the *data hiding* and *the retrieval phase*. The data hiding phase consist of the RDH method which is used to hide the data in different format and can be extracted using the different technique. The *Region separation method* is used to hide the secret data in the different region of the image and so ,only the authorized user can decrypt and access the data. The ICT and IWT methods are used to hide the data in the image so that the original image is not altered. The mechanism used to protect the loss of data by cropping the stegno image that contains the data is RDH so that image cannot be cropped. The security level for the data is increased in this kind of system.

2. RELATED WORKS

On the part of stegnography 'n' number of works has been developed. In the encryption phase the data carrying pixel should be hidden. Our proposed work provide these to increase the secrecy of the data. Katzenbeisser, S. and Petitcolas, F.A.P., [1] proposed Information Hiding Techniques for Steganography and Digital Watermarking. It helps in copyright protection. M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa [2] proposed Integer Wavelet Transforms in Colored Image-Stegnography. The frequency and the location information is captured. Guorong Xuan et. al [3] proposed Distortionless Data Hiding Based on Integer Wavelet Transform. It provides. Shejul, A. A., Kulkarni, U.L.,[4] proposed A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform. cropping case used here preserves histogram of DWT coefficients after embedding. It can be used aldo to prevents histogram based attacks. Masud, Karim S.M., Rahman, M.S., Hossain, M.I. [5] proposed A New Approach for LSB Based Image Steganography using Secret Key. It is difficult to extract the hidden information knowing the retrieval methods. The Peak Signal-to-Noise Ratio (PSNR) measures the quality of the stego images and also gives better result. This is because of very small number of bits of the image.

Xie, Qing., Xie, Jianquan., Xiao, Yunhua. [6] A High Capacity Information Hiding Algorithm in Color Image. The security is much higher because the visual effect of image is not affected. Sachdeva, S and Kumar, A., [7] Colour Image Steganography Based on Modified Quantization Table. The cover image is divided into blocks and DCT is applied to each block. IDCT is applied to produce the stego image which is identical to cover image. Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J. [8] Multi-bit Bitwise Adaptive Embedding Algorithms with Minimum Error for Data Hiding. The system provides embedding algorithms that results in minimum error and it is suitable to hardware implementation due to it is based on logic, algebraic, and bit operations. Roy, S., Parekh, R., [9] A Secure Keyless Image Steganography Approach for Lossless RGB Images. The system authentication is provided and Storage capacity is increased. Hiding the information provides minimal Image degradation.. Mandal, J.K., Sengupta, M., [10] Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF). It shows better performance in terms of PSNR and fidelity of the stego images.

3. SYSTEM ARCHITECTURE

The system architecture or the design gives value of revealing the process that is done during the experimental works. The sender first authenticates himself to enter the system which is known as the login details that is stored in the database and the takes the image that he wants to transmit and collects the data that are important as a cover message and then encrypts the image. A key is provided. This stegno image will be transmitted over the networks and it will be recovered in the receiver end. Then the original secret data is said to be constructed and then the original image and hidden data can be regained by using the absolute keys.

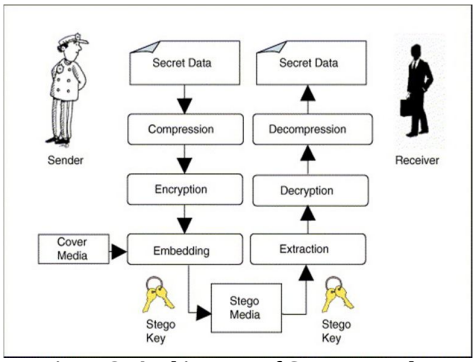

Figure 2: Architecture of Steganography

4. RESEARCH PROPOSAL

STEP 1: CLASSIFYING INTO PIXELS

Here ICT and IWT are used to split the image into pixels. A Integer cosine transform (ICT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. An Integer wavelet transform (IWT) is any wavelet transform for which the wavelets are discretely sampled. Temporal resolution is maintained. The pixels are initially classified and then data for each of the pixel is embedded. This increases the confidentiality of the data that is to be hidden and transmitted.

Algorithm 1: ICT

The integer cosine transform (ICT) is an approximation of the discrete cosine transform.Integer arithmetic mode is used in implementation. It promotes the cost and speed of hardware implementation.

```
if (temp == 255)
{
  i++;
  int value = ICT[i],  length = ICT[i];
 for(j=0; j<length; j++)
 {
   pixel[k] = value;
   k++;
```

Algorithm 2: IWT

This algorithm is used to reduce the space of usage. This part is also associated with classifying the pixels of an image. The area without a pixel value or RGB value is skipped.

```
IWT( )
while( h >= minWaveLength )
 {
double[ ] iBuf = new double[ h ];
 for( int i = 0; i < h; i++ )
{
 iBuf[ i ] = arrHilb[ i ];
double[ ] oBuf = _wavelet.forward( iBuf );
}
 for( int i = 0; i < h; i++ )
{
arrHilb[ i ] = oBuf[ i ];
 h = h >> 1;
 level++;
```

STEP 2: GENERATING RANDOM NUMBERS AT THE CORNERS

Here a new least significant bit embedding algorithm for hiding secret messages in non adjacent pixel locations of edges in the image is proposed. Here the messages are hidden in regions which are least like their neighboring pixels so that an attacker will have less suspicion of the presence of message bits in edges, because pixels in edges appear to be much brighter or dimmer than their neighbours. Edges can be detected by edge detection filters . For a 3x3 window Laplacian edge detector has the following form.

$$D=8x_5 - (x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9)$$

Where x_1 , x_2 , x_3 , x_4 , x_5 , x_6, x_7, x_8, x_9 and are the pixel values in a sliding 3x3 window scanning from the top left to bottom right with center pixel value.

x= D will become positive when the center pixel x is brighter is brighter than its neighbours and vice versa. The disadvantage of LSB embedding is that it creates an imbalance between the neighbouring pixels causing the value of D to change. Here this imbalance is avoided by flipping the gray-scale values among 2i-1, 2i and 2i+1. D after LSB embedding is not different from the old value of D before embedding. The various strengths of this scheme are that an

attacker will have less suspicion to the presence of message bits in edges because pixels in edges appear to be either much brighter or dimmer than their neighbours and it is also secure against blind steganalysis. In order to ensure that the neighbouring pixels in the window are not changed by Laplacian edge detectors, we apply the edge detection filter in non overlapping window only. It also limits the length of the secret message to be embedded. The proposed algorithm random edge LSB (RELSB) embedding uses least significant bit embedding at random locations in nonadjacent edge pixels of the image.

Algorithm 3: LSB

```
hideMessage()
{
string message = messageTextField.getText();
boolean displayInWhite = checkBox.getState();
if(originalImage == null)
{
Frame f = new Frame();
MessageDialog notL = new MessageDialog(f, "Error",
"Please load an image to hide the message");
notL.pack();
notL.show();
return;
}
if (message.length() == 0 || message.length()>40)
{
Frame f = new Frame();
MessageDialog mdialog = new MessageDialog(f, "Error",
"Please use a valid message (less than 40 letters)");
mdialog.pack();
mdialog.show();
return;
}
}
```

Figure 3: HBC Technique

A technique called *Pseudo Random Generation* is used here for generating numbers at the corners of image**.** It is for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the *PRNG*'s state, which includes a truly random seed. Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom numbers are important in practice for their speed in number generation and their reproducibility.

Algorithm 4: PSEUDO RANDOM

G = (i, j) = mod [p(i, j) + e(i, j) , 256]

N1=row,N2=column
e.g.:100x200
N1=100,
N2=200

STEP 3: ENCRYPTION

Encryption is a common technique to uphold image security.An image can be grasped and data can be retrieved if it is in original form. Hence Block Based transformation algorithm is used to encrypt confidentially.

Algorithm 5: BLOCK BASED TRANSFORMATION

```
While I < NoBlocks
R = RandomNum between (zero and NoBlocks -1)
If R is not selected Then
Assign location R to the block I
I +=1
Else
If SEEDALTERNATE = 1 Then
seed = seed + (HashValue1 Mod I) +1
SEEDALTERNATE = 2
Else
seed = seed + (HashValue2 Mod I) + 1
SEEDALTERNATE = 1
Randomize (seed)
End If
Else
Number-of-seed-changes += 1
If Number-of-seed-changes > 500,000 then
For K = 0 to NoBlocks -1
If K not selected then
Assign location K to Block I
I=I+1
End if
Next K
End if
End if
```

STEP 4: TRANSMISSION

The encrypted image is transmitted to the receiver. The keys that are responsible for the retrieval of image is to be sent to the receiver. The image and the hidden data could be retrieved only if all the four keys were properly matched.

STEP 5: RETRIEVING ORIGINAL DATA

A content owner encrypts the original uncompressed image using an encryption key. Then by using least significant bits of the encrypted image is compressed. A data-hiding key is used to create a space to save some confidential information. If a receiver has the data-hiding key, then the image content can be retrieved. With the encryption key one can retrieve the image and not the confidential information. Data hiding key and encryption allowsa a user to retrieve both the original image and the confidential information. The data is not get lost by the authorized user by RDH at the corners.

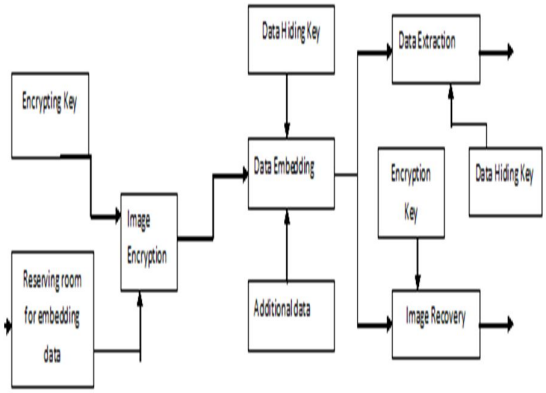

Figure 4: Proposed Architecture

Algorithm 6: RDH

```
pictureBox1.Image=Image.FromFile(EnImage_tbx.Text) ;
 if (saveFileDialog1.ShowDialog() == DialogResult.OK)
{
 saveToImage = saveFileDialog1.FileName;
 }
 else
  return;
  if (EnImage_tbx.Text == String.Empty || EnFile_tbx.Text
== String.Empty)
  {
   MessageBox.Show("Encryption information is
```

5. CONCLUSION

This project has proposed a novel scheme of scalable coding for stegno images. The data that get hidden in the image can be extracted by the intruders by using various techniques. This project used the various techniques like RDH,IWT,DCT,HBC to secure the data from the intruders. The Stegnanalysis methods can be used to retrieve the original data from the sender and the user can view the same quality of the stegno image as the original imgae has. The quality and the size is get maintained in this project. The HTML embedding can be used in the further future enhancement.

6. REFERENCES

[1] Katzenbeisser, S. and Petitcolas, F.A.P., (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London

[2] M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa, (2004) "Using Integer Wavelet Transforms in Colored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, pp. 75-.

[3] Guorong Xuan et. al, (2002) “Distortionless Data Hiding Based on Integer Wavelet Transform”, Electronics Lelters, Vol. 38, No. 25, pp. 1646-1648.

[4] Shejul, A. A., Kulkarni, U.L., (2011) “A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform”, International Journal of Computer Theory and Engineering, Vol.3

[5] Masud, Karim S.M., Rahman, M.S., Hossain, M.I., (2011) “A New Approach for LSB Based Image Steganography using Secret Key.”, Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 – 291

[6]] Xie, Qing., Xie, Jianquan., Xiao, Yunhua., (2010) “A High Capacity Information Hiding Algorithm in Color Image.”, Proceedings of 2nd International Conference on E-Business and Information System Security, IEEE Conference Publications, pp 1-4.

[7] Sachdeva, S and Kumar, A., (2012) “Colour Image Steganography Based on Modified Quantization Table.”, Proceedings of Second International Conference on Advanced Computing & Communication Technologies , IEEE Conference Publications, pp 309 – 313.

[8] Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J. Novel Multi-bit Bitwise Adaptive Embedding Algorithms with Minimum Error for Data Hiding. In Proceedings of 2010 Fourth International Conference on Network and System Security (NSS 2010), (Melbourne, Australia, 1-3 September 2010), IEEE Conference Publications, 306 – 311.

[9] Roy, S., Parekh, R., (2011) “A Secure Keyless Image Steganography Approach for Lossless RGB Images.”, Proceedings of International Conference on Communication, Computing & Security, ACM Publications, 573-576.

[10]] Mandal, J.K., Sengupta, M., (2011) “Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).”, Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301