ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

DATA EMBEDDING TECHNIQUE IN IMAGE STEGANOGRAPHY USING NEURAL NETWORK

Usha B A[1], Dr. N K Srinath[2], Dr. N K Cauvery[3]

Assistant Professor, Department of CSE, R V College of Engineering, Bangalore, India [1]

Professor and Head, Department of CSE, R V College of Engineering, Bangalore, India [2]

Professor, Department of ISE, R V College of Engineering, Bangalore, India [3]

Abstract- The steganography is the process of concealing one medium of information within another. There are lots of techniques available to achieve steganography like least significant bit insertion method and transform domain technique. This project implements the new method of steganography whose foundation lies on neural network. The amount of data that can be hidden inside the cover image chosen depends on the properties of the image like number of noisy pixels. The neural network based image steganography ensures that quality and size of the image remains same after embedding the data. Neural network based steganography has wide applications today in military operations, protection of data alteration, media database systems and secret data storing.

Keywords- Neural Network, steganography, LSB insertion, transform domain.

I. INTRODUCTION

In this modern era, computers and the internet are major communication media. They connect different parts of the world and have made the world one global virtual world. As a result, people can easily exchange information without distance being a hindrance. However, the safety and security of long-distance communication is an important consideration. The need to solve this problem has led to the development of steganography schemes. Steganography is a strong security tool that provides a high level of security. But this is particularly when it is combined with encryption. In image steganography image is one of the most popular cover objects. Schemes like LSB insertion and JPEG steganography makes the steganalysis very simple for the opponent. The increasing need of better methods of image steganography has motivated this new concept. The neural network based steganography is very effective to hide the secret data in the images.

II. RELATED WORK

a) LSB Insertion Method

This is the most popular technique when dealing with images. The simplicity of this method is at the cost of compression which is inherently lossy. The traditional LSB [1] technique takes into account every possible bit. 3 bits are safeguarded in every pixel since there is a option to use red, green or blue. The method works by choosing last bit to store the information. For enhancing security encryption technique is used. This security is achieved at the cost of added complexity. This method uses two popular techniques Rivest, Shamir, Adleman (RSA) algorithm and Diffie Hellman algorithm to encrypt the data. LSB insertion is of prime significance with a gray scale palette. The challenge in LSB technique is the issue of corruption. This means that the integrity of the message is not really taken into consideration. The decoding is relatively simple making it less secure.

b) Transform domain techniques

This technique embeds the hidden information in the transform domain. Image samples are decorrelated .To achieve this, key is used. This technique enhances the value of transmission coefficients significantly. The benefit with this method is it becomes easy to embed more data.DCT [2] values for the blocks are computed. A quantization technique is used to embed the hidden data. Quantization is another technique that comes handy to retrieve information in a secure manner. The decoding process also involves a

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

key which is same as encoding process. The key is very important in this process because its unavailability at decoder makes the retrieval of information impossible.

III.PROPOSED METHOD IMPLEMENTATION

a) Sender module

The sender module takes the cover image and secret data to be hidden as the input. It performs the encryption of secret data using a password chosen by sender . By embedding bits in the LSB of noisy pixels it hides this encrypted secret data.

b) Encryption

Encryption includes a message or a file encrypting. Encryption involves converting the message to be hidden into a cipher text. Encryption can be done by passing a secret key. Secret key can be used for encryption of the message to be hidden. It provides security by converting it into a cipher text. This makes it difficult for hackers to decrypt. Greater security is added if the message is password protected. Then while retrieving message, the retriever has to enter the correct password for viewing the message.

AES [3] is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES [4] in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size.

c) Salient Features

•The cipher key is expanded into a larger key. This is later used for the actual operations

•The round Key is added to the state before starting the with loop

•The Final Round () is the same as Round (), apart from missing the Mix Columns () operation.

•During each round, another part of the Expanded Key is used for the operations

•The Expanded Key shall always be derived from the Cipher Key and never be specified directly.

d) Hiding Module

Hiding message is the most crucial module of steganography. It involves covering the message into the cover text. Each pixel typically has three numbers, one each for red, green, and blue intensities. These values often range from 0-255. In order to hide the message, data is first converted into byte format. It is then stored in a byte array. The message is encrypted. Then it is embedded each bit into the LSB position of each pixel.

e) Neural Networks

Unlike von Neumann model computations [5], artificial neural networks do not separate memory and processing. They operate via the flow of signals. It happens through the net connections. It is somewhat similar to biological networks. These artificial networks may be used for prediction. Other applications include they can be trained via a dataset. A biological neural network [6] is composed of neurons with same functionality.

Neural network algorithm

Step 1: The cover image entered by the sender is stored as original image which is a byte array which contains the bytes of all pixels in the image.

Step 2: Block size and difference should be chosen by sender.

Step 3: The original image is divided into blocks based on the block size.

Step 4: The blocks are copied onto a temporary array list which are in turn stored as dictionary values.

Step 5: A background worker (thread) is used to operate on dictionary values. The background worker can only act on one dictionary at a time.

Step 6: Find the highest value in dictionary using linq and the index of that will be the noisy pixel index.

Step 7: Check for the repetition of this highest value, if repetition occurs then discard that pixel and check for next highest value.

Step 8: Repeat step 4 to step 7 for all the blocks.

Step 9: The file name length of the secret data file, secret file content length, ASCII encoded secret file name, secret file content in byte array are all encrypted using AES encryption based on the key chosen by sender.

Step 10: The AES encrypted bits are embedded into the LSB of this noisy pixel.

Step 11: The back propagation is done by checking for non-ambiguousness in embedding the data. If we find any ambiguity then that noisy pixel will be discarded.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Step 12: The original image with hidden data is sent to the receiver in a secure manner.

Step 13: The receiver should perform the reverse procedure to find the noisy pixel and extract LSB bits from that.

Step 14: The encrypted secret bits are decrypted using the advanced decryption algorithm with the key that is shared between the sender and receiver.

Step 15: Stop

Receiver Module

The receiver module takes the cover image with the hidden data as the input. The encrypted secret data is then retrieved by applying suitable algorithm.Thesecretdata is obtained by using AES decryption algorithm.

Retrieve

It involves retrieving the embedded message from the file. After retrieval the message has to be converted into original message or file. The read data will be in the bytes format. It is essential that the message is in the suitable output file format.

Decryption

Decryption involves converting the cipher text into decrypted format. Decryption involves use of a secret key. It enhances security by converting the cipher text, into the original data message or file. The robustness of the system can be increased further if the message is password protected. Then while retrieving message, the retriever has to enter the correct password for viewing the message.

IV.EXPERIMENTAL ANALYSIS

The image quality of stego image compared to the original image is measured using Peak Signal to Noise Ratio (PSNR) in dB. At least 30 images must be embedded with different sizes. It would have been tedious to work in designed software. So, to automate these test cases a test tool is created which would take all of these cover images in a serial fashion and based on the embedding capacity it automatically creates a file whose length is the full embedding capacity of the image and then the image was embedded and mean square error was calculated and PSNR was found out in all these cases. Tabulated results shown in table 4.

Fig:Jelly bean

Jelly fish	256 x 256		306 x 468		512 x 512	
% embed	PSNR	MSE	PSNR	MSE	PSNR	MSE
0.1	42.5254	3.6353	42.5254	3.5982	42.5733	3.5954
0.2	39.5109	7.2776	39.5109	7.2147	39.5831	7.1576
0.3	38.4854	9.2159	38.4854	9.0156	38.6009	8.9741
0.4	38.4853	9.2161	38.4853	9.0158	38.6012	8.9734
0.5	38.4389	9.3151	38.4389	9.0151	38.6007	8.9745
0.6	38.3925	9.4153	38.3925	9.0153	38.6009	8.9741
0.8	38.3469	9.5145	38.3469	9.0145	38.6005	8.9749
0.7	38.3465	9.5155	38.3465	9.0155	38.6006	8.9747
0.9	38.3025	9.6123	38.3025	9.0144	38.6004	8.9751
1	38.2976	9.6232	38.2976	9.0154	38.6005	8.975

Table 4: MSE, PSNR values for different embedding capacities for 256x256,308 x 468, 512 x 512 resolution of a jelly fish image.

V.CONCLUSION

The neural approach to embed information satisfies a secure steganography. Neural approach adds the complexity for the hackers accessing and also presents high potentiality in defense operations. Neural Steganography is a powerful tool that enables people to communicate without possible eavesdroppers even knowing there is a form of communication.

Equally important are the ethical concerns of using steganography and steganalysis. Using steganographic techniques, software can easily transmit private user information without the user's permission or knowledge. Watermarks already an issue in the hosty disputed domain of digital rights management could be comprised by advanced steganalysis tools. Similar abuses of steganography and steganalysis can easily be enumerated. The amount of secret information that can be hidden is limited by the size of the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

image. The algorithm is not very effective for heavy multimedia content like video.

Future Enhancement

The secret message should be compressed or encoded before the hiding process takes place. This is important because in this way we will minimize the amount of information that is sent, and hence minimizing the chance of degrading the image. At the same time results of steganalysis can be used to change or improve embedding techniques. Since data hidden depends on the number of noisy pixels found this technique should be enhanced to hide large amount of data.

REFERENCES

[1] WaiWaiZir "Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR), Volume 2 Issue 1, January 2013.

[2] Sudhanshu S Gonge, Jagdish W Bakal , " Robust digital watermarking technique by using DCT and spread spectrum" International Journal Of Electrical, Electronics and Data Communication, ISSN (print): 2320-2084, volume – 1, issue – 2, 2013

[3] Fei Shao, Nanjing, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Second International Conference on Communication Software and Networks, 2010

[4] Thomas J. Watson Research Center, P. O. Box 218, Yorktown Heights, New York 10598, USA, "Data Encryption Standard its strength against attacks",IBM journal of research and development ,May 1994

[5] H. NortanRieley ," The von Neumann Architecture of Computer System", Computer Science Department California State Polytechnic University Pomona, California, September, 1987

[6] RafikBraham,James O Hamblen, "The design of a neural network with a biologically motivated architecture." ,IEEE transactions on neural network, September 1990