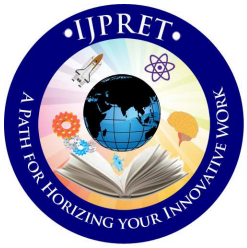
Research Article *ISSN: 2319-507X*
Geeta Shrivastava, IJPRET, 2013; Volume 1(8):663-672 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHY, STEGNOGRAPHY AND NETWORK SECURITIES

PROF.GEETA SHRIVASTAVA, PROF. SARIKA KSHIRSAGAR, NILESH SHRIVASTAVA

1. HOD, MCA Dept. JSPM's AIOCA, Pune, (MS), India.
2. Assistant Professor, JSPM's AIOCA, Pune, (MS), India.
3. Technical Leader, I Gate Corporation, Pune, (MS), India.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Cryptography and Steganography,
Data dictionary,
Gray level modification

Corresponding Author

Prof. Geeta Shrivastava

Abstract

In any communication, security is the most important issue in today's world. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Cryptography and Steganography. Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. In this paper, information security is achieved using the

Introduction:

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. In this paper, a combination of cryptography and steganography has been used to enhance embedding capacity of a steganographic channel by preprocessing the secret data and applying encryption technique over it to make it more robust against Steganalysis. The proposed work technique is limited to textual data only. Here the concept of Scrambled Letters, Dictionary Module has been used. All these concepts when applied together give a phenomenal embedding capacity. Typically, the message is embedded within another object known as a cover work, by tweaking its properties. So what this paper discussed is by improving this technique by applying encryption technique and then applying one compression technique so that an improved technique can send more text as compared to other traditional techniques and which is more robust and more secure against staganalysis. This technique is generic and can be applied to any form of textual data without any form of graphics like images or graphs. Once the data is preprocessed by using this technique it can be easily embedded in any steganographic cover medium by using any steganographic algorithm. In this we address the issue of embedding capacity of a steganographic channel. All existing techniques compress the secret data before embedding it in a cover medium to achieve higher embedding capacity. the secret data before even compressing it. He introduce this step to reduce the size of data set which would be compressed and finally embedded. To preprocess the data he introduces two techniques. One of his techniques is generic and can be applied to any form of textual data

Cryptography and Steganography:

cryptography is an effective way of protecting sensitive information. On the other hand Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Although the ultimate

goal of cryptography, and the mechanisms that make it up, is to encrypt information from unauthorized individuals. So, cryptography encrypts the message and converts it into cyphertext while Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. The advantage of steganography over cryptography is that stego image does not attract attention while plainly visible encrypted messages no matter how unbreakable will arouse suspicion. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Dictionary Module

The DM is a small database of words similar to a dictionary. But these words are stored in a sorted order, which is different from a normal dictionary. The sorting criteria are:

1. Alphabetical Order: Firstly all the words are stored in an alphabetical order.

2. Ending Letter: Secondly the words are sorted according to the letter with which they end but maintaining the alphabetical order. E.g. [Steganographic, Steganography]

3. Number of letters in a word: This sorted list is finally sorted based on the number of letter they have maintaining the above two criterion.

This technique is a generic technique and can be applied to any form of textual data, i.e. word processor file which has some text, some graphs and some images. By using this technique we only process the textual portion. The basic idea behind the dictionary approach is to process each word one after the other to represent it in as minimum letters as possible. When it mean processing each word, it mean skipping some letters from a word in a predetermined order, in such a way that the word can be properly regenerated, if we know which letters are skipped and from where. In the proposed algorithm we decide to skip alternate letters in a word.

To explain this following example is taken. Suppose we have a word 'Sarika'.

We keep the first and the last letter intact, while we delete the alternate letters within,

i.e. instead of 'Sarika' we can have 'S r k a'. As a result of this step we reduce the size of the data. We would only transmit 'S r k a' instead of the complete word 'Sarika'.

S	a	r	i	k	a

The original words to be transmit.

S		r		k	a

The words to be transmit according to DM.

Another example suppose we have a word 'Geeta' instead of transmitting whole world 'Geeta' we would transmit 'G e a".

G	e	e	t	a

The original words to be transmit.

G		e		a

The words to be transmit according to DM. DM takes the processed word and some parameters to uniquely identify the proper word. In case of the example discussed earlier we can recover 'Geeta' from 'G e a'using this module.

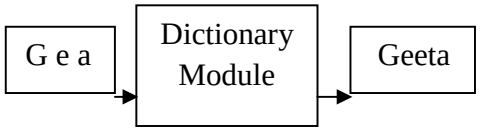


Fig. Dictionary Module

Now a technical detail of the DM has been discussed. Basically DM is a search algorithm which takes four parameters:

1. Length of the original word: This can be deduced form the processed word.

2. The Starting and the Ending letter of the processed word: This is the same as in the original word, e.g. G and a.

3. List of letters from the processed word: E.g. In case of ''G e a ', the list of letters would be [g,e,a]

4. Location of these letters: E.g. G is 1^{ST} , e is 2^{nd} & 3^{rd} , a is 5^{th} etc.

After having all these parameters, the DM conducts a search looking for words that satisfy this criterion. The outcome of this search is the original word. Thus we can regenerate the processed word based on the DM. The DM that we build had all the words listed in an Oxford Dictionary.

The concept of DM was inspired by the article posted on the Internet which said misspelled words can be interpreted properly as long as the first and last letters are correct and are in their proper place,

even though the letters in between can be scrambled or even missing.

Using this DM all the words of textual data can be processed. Then these processed words to be transmitted to sender instead of original words. At the receiving end original words can be retrieved from these processed words

Gray level modification (GLM) technique:

In 2004, Potdar et al. [7] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels.GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image. Initially, the gray level values of the selected pixels (odd pixels) are made even by changing the gray level by one unit. Once all the selected pixels have an even gray level it is compared with the bit stream, which has to be mapped. The first bit from the bit stream is compared with the first selected pixel. If the first bit is even (i.e. 0), then the first pixel is not modified as all the selected pixels have an even gray level value. But if the bit is odd (i.e. 1), then the gray level value of the pixel is decremented by one unit to make its value odd, which then would represent an odd bit mapping. This is carried out for all bits in the bit stream and each and every bit is mapped by

modifying the gray level values accordingly.

Results & Analysis With the Example

Preprocessing of data :

Suppose we have to send

"Abacus Institute Of Computer Applications is the best college"

According to ASCII coding we have to send it in standard 8 bit codes. There are total 66 alphabets in this sentence including

a=1	**b=2**	**c=3**	**d=4**
e=5	f=6	g=7	h=8
i=9	j=10	k=11	l=12
m=13	n=14	o=15	p=16
q=17	r=18	s=19	t=20
u=21	v=22	w=23	x=24
y=25	z=26		

space therefore it will use 60*8=480 Bits. Now we will calculate how many bits will it consume in our proposed technique.When we apply preprocessing of bits according to Potdar *et al* the given sentence will become

"A a us I s i u e Of C m u t r A p i a i ns is t e b s t c l e e"

Now we will send this preprocessed data for Encryption.

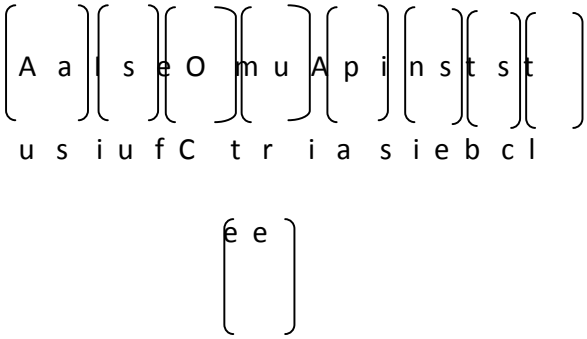
Data Encryption using Matrix Encoding.

First assign values to alphabets

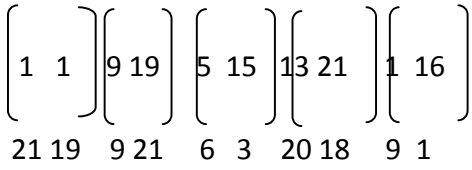
Now arrange the preprocessed text

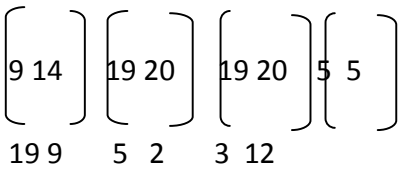
"A a us I s i u e Of C m u t r A p i a i ns is t e b s t c l e e"

In 2*2 matrix



Now replace each alphabet with it corresponding value assigned.





Now we will multiply each matrix with the coding matrix(Key) which is known only to sender and receiver.

Here coding matrix is $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

Now multiply this coding matrix with all the above 2*2 matrices obtained above

$$\begin{pmatrix} 1 & 1 \\ 21 & 19 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 59 & 61 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 15 \\ 6 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 35 & 25 \\ 12 & 15 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 19 \\ 9 & 21 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 47 & 34 \\ 51 & 39 \end{pmatrix}$$

$$\begin{pmatrix} 13 & 21 \\ 20 & 18 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 55 & 47 \\ 56 & 58 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 16 \\ 9 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 33 & 18 \\ 11 & 19 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 14 \\ 19 & 9 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 37 & 32 \\ 37 & 47 \end{pmatrix}$$

$$\begin{pmatrix} 19 & 20 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 59 & 58 \\ 9 & 12 \end{pmatrix}$$

$$\begin{pmatrix} 19 & 20 \\ 3 & 12 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 59 & 58 \\ 27 & 18 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 5 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 15 & 15 \\ 2 & 1 \end{pmatrix}$$

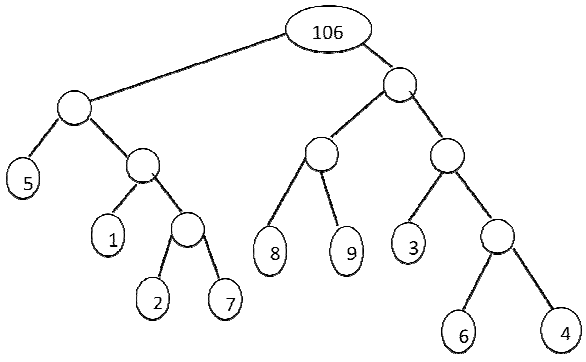
Now data transmitted will be in form

3 3 59 61 47 34 51 39 35 25 12 15 55 47 56 58 33 18 11 19 37 32 37 47 59 58 9 12 59 58 27 18 15 15

Symbol	Frequency
1	12
2	5
3	8
4	4
5	15
6	2
7	5
8	5
9	6
Space	32

We will apply Huffman coding on this data to construct a Huffman Tree

The Huffman tree generated for the above data is shown by figure



Codes according to Huffman Tree

1	010
2	0101
3	111
4	1100
5	00
6	1010
7	0101
8	101
9	110
space	11

3 3 59 61 47 34 51 39 35 25 12 15 55 47 56 58 33 18 11 19 37 32 37 47 59 58 9 12 59 58 27 18 15 15

This data to be send according to Huffman code

111 11 111 00110 1010010 11 11000101 11 1111100 11 00010 11 111110 11 11100 11 010100 11 0100101 11 01000 11 0000 11 11000101 11 001010 11 00101 11 111111 11 010101 11 010010 11 010110 11 1110101 11 1110101 11 1110101 11 11000101 11 00110 11 00101 11 110 11 0101010 11 11110 11 00101 11 01010101 11 010101 11 01011 11 01000

According to ASCII code we will use 480 bits to send this data .

According to our technique we will have to send 261 bit to send this same amount of data.

So we got (261/480)*100=54.37 % less

Through our above technique the embedding capacity of transmission medium of Steganographic technique has improved. This technique has twin benefits of Encryption and Steganography.Theoretical results show that it has improved the embedding capacity of transmission medium to 15-25 % (average).

7. Conclusion and Future Work:

In this paper, Steganography and Cryptography bas been discussed. It proposed a methodology to improve the embedding capacity of transmission medium of Steganography with the use of combining features of Steganography and Cryptography both.It shows how a data can be send more securely by applying some of Encryption techniques over it before sending it to the receiver using any of Steganographic Technique. There has been improvement in the method proposed by Potdar et al. In preprocessing of data has been applied using Potdar et al and then Matrix encoding has been applied to secure the data. After that Huffman Encoding is has been applied to compress the size of data to be sent. By this technique not only its able to reduce the number of bits to be used to send the data but also make it more robust against steganalysis. Theoretical results show that it has can improved the capacity of transmission medium to 15-25% (average).But the efficiency of this proposed method may vary with the length and content of textual data.

References:

1. www.wikipedia.com

2. Bloisi ,Domenico., Iocchi, Luca.,"Image Based Steganography and Crytography

3. Soumeyendu Das, Subhendu Das , Bijoy Bandhopadhyay , Sugata Sanyal, "Steganography and Steganalysis:Different approaches".

4. Willaim Stalling, "Cryptography and Network Security Principles" Fourth Edition PHI Indian Edition

5. Potdar, V.,Chang E. Gray level modification steganography for secret communication. In IEEE International Conference on Industria l Informatics. pages 355–368, Berlin, Germany, 2004. .

6. 6.Potdar, Vidyasagar M., Han, Song., Chang, Elizabeth.,"Dictionary Module and UDC:Two new approaches to of a Steganographic Channel.3rd IEEE International Conference on Industrial Informatics (INDIN) Enhance Embeeding Capacity Perth,Australia 10-12 August 2005.

7. L.Y. Xiang, X.M. Sun, G. Luo, C. Gan, "Research on steganalysis for text steganography based on font format", The 3rd International Symposium on Information Assurance and Security, Manchester, United Kingdom, pp.490–495, 2007.