International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Steganography Using the Twelve Square Substitution Cipher and an Index Variable

Aparna Saxena[1], Munmun Ghosal[2]

[1,2] G. H. Raisoni College of Engineering. & Management Pune, Maharashtra, India

Abstract: ***The security during data transmission has become of prime importance in the world, including India. It has significant impact on internet. This paper proposes an approach using both cryptography and steganography.In this first we encrypt the secret message using a techniques called twelve square substitution method to obtain cipher text .Thus cipher text is embedded in the carrier image using index variable to perform secret communication between the sender and the reciever.Due to this use of both cryptography & steganography this approach is stronger .This algorithm will be implemented using Mat lab.***

Keywords: Crtography, steganography, twelve square cipher.

1. Introduction

Steganography is a technique of secret communication in which the information to be transmitted is transmitted by embedding into other object .The word steganography is basically a Greek word meaning covered writing steganography can be done using image, audio & video carrier. Among these steganography technique image steganography is more popular as image is least distorted .

The change due to image steganography is so small that human eye cannot suspect any secret code embedded due to limited resolution power of human eye. Information is embedded in image using an index variable. In index variable value can be 0,1 or 2.[1]

2. Existing Image steganography Methods

Various methods have been proposed for image steganography.In this image is first encrypted & then secret information is embedded in LSBs & for secure process entropy & correlation value of stego image & original image should be same . Important thing while, steganography is that, visible properties of carrier should not be changed a lot.

LSBs methode is the simplest & widely used method for steganography because it change bit from either 1 to 0 or vice versa due to which there is hardly any change in the appearance of the color of that pixel as there are 256 color combination .If the information to be hidden in file using LSBs are larger then it may become noticeably distorted.

Steganography using LSBs method is being proposed by Mohmmad Ali Bani younes et.al. .H. Motammeni et.al proposed labeling method in steganography in which different color are labeled dark place in the image are recognized & than text is inserted at the dark places.

P Mohan Kumar & D Roopa proposed a steganography method for tamper-proofing they have suggested an application that the photographer working in enemy area can use this method to send the spry photographs. Encryption of secret message is done using a Twelve square substitution method & then this cipher text is inserted at 6^{th} & 7^{th} or 7^{th} & 8^{th} or 6^{th} &8^{th} bit location of bytes of image depend on different value of index variable.

3. The Twelve Square Substitution Cipher

Twelve square substitution cipher algorithm is an extended or improved version of six square subsitution cipher. Six square subsitution has been used only for alphabets & special character where not included in it. So to overcome this drawback twelve square subsitution has been used. Twelve square subsitution can be used for alphabets, digits & special character thus less susceptible to frequency attacks .It contain 5 X 5 matrices containing letter of alphabets to fit into square containing letters of alphabets (omitting Q) to reduce the alphabet to fit into the square as shown in table 1 and other 6X 7 matrics containing digit & special characters as shown in table 2. Both tables are arranged in square.

Plain Text and Cipher Text (Alphabets)

Square-1	**Square-2**	**Square-3**
a b c d e	f g h I j	k l m n o
f g h I j	k l m n o	p r s t u
k l m n o	p r s t u	v w x y z
p r s t u	v w x y z	a b c d e
v w x y z	a b c d e	f g h I j
Square-4	**Square-5**	**Square-6**
g m r i t	a b c d e	a b c d e
a b c d e	f h j k l	f h j k l
f h j k l	g m r i t	n o p s u
n o p s u	n o p s u	v w x y z
v w x y z	v w x y z	g m r i t

Process to arrange table 1:-
Square 1: Twenty five alphabets excluding Q are arranged in 5row and 5 columns.
Square 2:- It is formed by placing first row from square 1 in fifth rows and other row one position upward.
Square 3:-It is formed by placing first row of square 2 in 5^{th} row and other row one position upward.
Square 4:- It is formed by putting GMIRT in first row & remaining alphabets in next row.
Square 5:- It is formed by putting first row of 4^{th} square to third row.

Square 6:- similarly it is formed by putting first row of square 4 to fifth row.

Table 2: Plain Text And Cipher Text (Digits And Special Characters)

Square-7	Square-8	Square-9
0123456	789`~!@	#$%^&*(
789`~!@	#$%^&*(	)_-+={[
#$%^&*(	)_-+={[	}];:“‘\
)_-+={[	}];:“‘\	|<,>.?/
}];:“‘\	|<,>.?/	0123456
|<,>.?/	0123456	789`~!@
Square-10	**Square-11**	**Square-12**
06!&+;<	17@*=:,	17@*=:,
17@*=:,	28#({“>	28#({“>
28#({“>	06!&+;<	39$)[‘.
39$)[‘.	39$)[‘.	4`%_}\?
4`%_}\?	4`%_}\?	5~^-]| /
5~^-]| /	5~^-]| /	06!&+;<

Process to arrange table 2:-
Square 7:- It is formed by arranging numerals and special characters from a standard laptop in six row and seven columns
Square 8:-It is formed by placing first row of square 7 in sixth rows.
Square 9:-It is formed by placing first row of square 8 in sixth rows.
Square 10:- It is formed from square 7 by arranging row element in columns.
Square 11:- It is formed from square 10 by placing first row of square 10 in third row places.
Square 12:- It is formed from square 10 by placing first row of square 10 in sixth row places.

Process to convert plain text to cipher text:-

Plain text is read from left to right. If first character is alphabet refer table 1.For numbers & special character refer table 2.

If first variable of plain text is alphabet it will be in first square and its cipher text will be on same row and column location of square 4 ,second alphabet will be in second square and its cipher text will be on same row and column location of square 5 and for third alphabet of plain text will be in third square 3and its cipher text will be in same row and column of square 6.Similarly `for 4 alphabet plain text will be in square 1& cipher text will be in square 4 and so on.

If the plain text is character refer table 2. for first Character or digits its plain text will be in Square 7 & cipher text will be in same position of Square 10 .For second character its plain text will be in square 8 and cipher text in square 11 .For third character or digits plain text will be in square 9 and cipher text in Square 12.and same process repeat for further text.
For example:
Plain Text:-
Hi how are you
Cipher text:-
addgh xlyz cd rlo vyz l

4. Embedding Process

Process for embedding Secret message into an image is as explained below:-
1) Convert the carrier image into binary form. Each pixel is 1 byte.
2) Convert Cipher text of secret message into bytes and calculate number of bytes (i.e., n).
3) Divide n by 3 ,say it is P (index variable)

If P = 0 hide data at 6^{th} and 7^{th} bit location of carrier.
If P = 1 hide data at 7^{th} and 8^{th} bit location of carrier.
If P = 2 hide data at 6^{th} and 8^{th} bit location of carrier.
Value of P Keep on changing from 0 to 2.first value depends on number of bytes.

Example:-
Suppose the cipher text to be sent is 11001010 01001010 10110110 10111011. This data is 4 bytes So n = 4 and p =1.Suppose the different bytes of the digital image are A, B, C, D etc, from table 3 it is seen that in byte A of the carrier file we embed the data bits 11 in 7^{th} and 8^{th} bit locations, next value of P become 2 .We embed the next data bits 00of byte B in 6^{th} and 8^{th} bit location, next p = 0 now we embed two bit 10in 6^{th} and 7^{th} bit location and so on .

Table 3: Byte Selection Using Index Variable

Carrier File Byte	Operation	Location	Index Variable,P
Byte A	Embed (11)	7^{th} and 8^{th}	1
Byte B	Embed (00)	6^{th} and 8^{th}	2
Byte C	Embed (10)	6^{th} and 7^{th}	0
Byte D	Embed (10)	7^{th} and 8^{th}	1
Byte E	Embed (011)	6^{th} and 8^{th}	2
Byte F	Embed (01)	6^{th} and 7^{th}	0
Byte G	Embed (10)	7^{th} and 8^{th}	1
Byte H	Embed (10)	6^{th} and 8^{th}	2
So on			

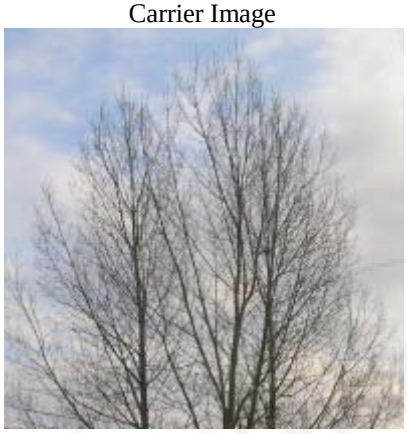
5. Proposed Algorithm

Step 1- Transform the carrier image into binary.
Step 2- Apply the Twelve Square Cipher to get the Cipher text of the secret message.
Step 3- Convert the cipher text to binary.
Step 4 - Make sure that the length of carrier image is sufficient enough to conceal the cipher text.
Step 5- cipher text is embedded into the cover image as discussed in the embedding process.
Step 6- Send the resultant image to receiver.
Step 7- Receiver applies the reverse process what sender has done and gets the hidden information.

Carrier file length should be 4n bytes .n bytes is the length of cipher text of secret message so to hide every one byte we require 4 carrier byte because every byte can hide 2 bits only.
Characteristics for good Steganography are as follows:-
1) It should be able to conceal a good amount of payload.
2) It should not be vulnerable to exhaustive search attacks.
3) The degradation in, quality of stego image should not be noticeable.
4) It should provide two level of security

6. Expected Results

Carrier Image



Plain Text
Hi how are you

Cipher Text
addgh xlyz cd rlo vyz l

After Embedding

Received Image

For different types of image this system should work .Carrier Image should be same as image after embedding data and there should not be any change. Data should be easily obtained at the receiver.

7. Conclusion

This algorithm provides two level of security one at stegnography and other at cryptography. With the use of index variable this algorithm becomes stronger because in this position of secret data keep on changing for every byte. So for intruder it is difficult to steal the data. and even the image quality remain same after embedding.

References

[1] Mohammad Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", International Journal of Computer Science and Network Security, Vol 8, No 6,2008, pp. 247-254.
[2] Ross J. Anderson and Fabian A.P. Petitcolas, "On the Limits of steganography", IEEE Journal of selected Areas in communication Vol.16, No.4, 1998, pp. 474-481.
[3] H. Motameni, M. Norouzi, M.Jahandar and A. Hatami, "Libelling method in Steganography", Proc. of world academy of science engineering and technology, Vol. 24, 2007, pp.349-354.
[4] P.Mohan Kumar and D. Roopa, "An Image Steganography Framework with improved Tamper Proofing", Asian Journal of Information Technology, Vol.6,No.10,2007 pp.1023-1029
[5] Xinpeng Zhang, Shuozhong Wang and Zhenyu Zhou, "Multibit Assignment Steganography in Palette Images", IEEE Signal Processing Transactions, Vol.15, 2008, pp. 553-556.
[6] Po Yuch Chen and Hung Ju Lin, "A DWT Based Approach for Image Steganography", International journal of Applied Science and Engineering, Vol.4, No.3, 2006, pp. 275-290.