STEGANOGRAPHY ALGORITHM USING ENCRYPTED SECRET MESSAGE

Gaurav Bora*

Rohinee Deshmukh*

Shrini Patel*

Sagar Phaphale*

Abstract

Security is the major issues for transmission of messages or any media files containing critical information. In this paper we are using LSB method and have modified the idea of Play fair method into a new platform where we can encrypt or decrypt any file.A secret key is entered by the user during encryption which is used at time of decryption. In this paper we propose technique for encryption of text into a cover image. For hiding secret message in the coverfile we have inserted the 8 bits of each character of encryptedmessage file in 8 consecutive bytes of the cover file. We proposethat our new method could be most appropriate for hiding anyfile in any standard cover file such as image, audio, video files.Because the hidden message is encrypted hence it will be almostimpossible for the intruder to unhide the actual secret messagefrom the embedded cover file. This method may be the most
Secured method in digital water marking.

Keywords –Steganography, Encryption, Decryption, Key.

* Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India

I. INTRODUCTION

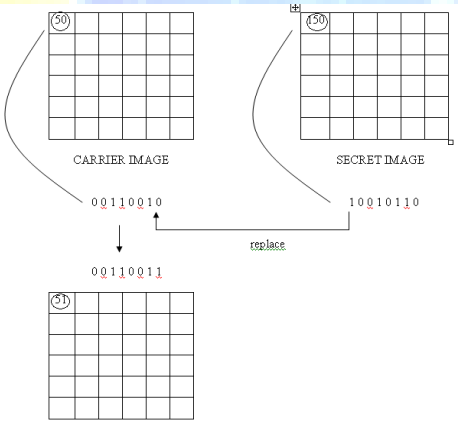
We insert the encrypted secret message inside the standard cover file (CF) by changing the least significant bit (LSB).

The already proposed different methods for embedding SM into CF but there the SF was inserted as it is in the CF and hence the security of steganography was not very high. In the present work we have basically tried to make the steganography method more secured. It means even if someone can extract SM from CF but he cannot be able to decrypt themessage as he has to know the exact decryption method. In our

Present work we try to embed almost any type of file insidesome standard cover file (CF) such as image file (.JPEG or.BMP) orany image file inside another image file. Here firstwe will describe our steganography method for embedding any

Type of file inside any type of file and then we will describe theencryption method which we have used to encrypt the secret

Message and to decrypt the extracted data from the embeddedcover file.



In our project we are changing LSB of the cover file with the MSB of the secret message as shown in the above figure. After the embedding the image distortion is very less because we are changing only the non-significant bits. Also we are compressing the original message if the message size exceeds the cover file size. Our method is totally key based one can get the original only if he has the key.

Section II represents the Literature Survey

Section III represents the Mathematical Model that describes the input, output functionalities along with the success and failure cases.

Section IV represents the System Design

Section V contains the implementation details of our system.

Section VI concludes this paper.

II.LITERATURE SURVEY

Hidden messages in waxtablets: in ancient Greece, people wrote messages on the wood, and then covered it with wax so that it looked like an ordinary, unused tablet. Hidden messages on messenger's body: also in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved head, hidden by the growth of his hair, and exposed by shaving his head againIn the 20th century, invisible inks where a widely used technique. In the Second World War, people used milk, vinegar, fruit juices and urine to write secret messages. WhenHeated, these fluids become darker and the message could be read. **Giovanni Batista Porte** described how to conceal a message within a **hardboiled egg** by writing on the shellwith a special ink made with an ounce of alum and a pint of vinegar.

III. MATHEMATICAL MODEL

1. Consider s is the system with set of parameters.

S= {i,o,d,f}

Where,

s= steganography system.

i=input file

o=output file

f=functions.

2. Now consider i is the set of input files

i= {i1,i2,i3,…..ii}

i1 ={mi|m is the original message}

m={.txt, .jpg,bmp}

i2={ni|n is the cover file}

n={.jpg, .mp3, .txt}

3. Now consider the function f1 and f2 are the inputs.

f1(m)=s1;

f2(n)=s2;

s1={mr|(mr)'}

s2={cr|(cr)'}

Where,

mr : message received.

(mr)': message not received.

cr : cover file received.

(cr)': cover file not received.

4. Now consider the function f3 is the set of inputs

- f3(m,n) =r

Where,

r : return type

r= {1|0}

if

r=1, then n>m

r=0, then n<m

5. Now f4 is the function for validation of size of the original message and the cover file.

- f4 (m,r)=mc.

Where,

mc =compressed original message.

6. Now function f5 is to embed inputs

- f5 (mc,n)=sf

Where,

sf =stego file.

7. Now function f6 is to generate key

- f6(sf)=sk

Where,

sk =stego file with key.

8. Now function f7 is to confirm key

- f7 (sk) =s3.

s3= {sr| (sr)'}

Where,

sr= stego file received.

(sr)'=stego file not received.

9. Now function f8 is to validate key

- f8(sf,k)=s4

Where,

sf is the stego file,

k is the key.

s4= {kc| (kc)'}

Where,

kc is key correct.

(kc)' is key incorrect.

10. Now function f9 is to separate the stego file.

- f9=(sk)={mc,n}

11. Now the function f10 is to obtain original message from the compressed message.

- f10(mc)= d

Where,

d= {ds| (ds)'}

ds=decompression successful

(ds)'=decompression not successful

12. Now ss , the output is given as

o= {m}

Where,

o is the output i.e. m which is the original message.

13. The set of dead states is given as,

d= {(cr)', (mr)', (sr)', (kc)', (ds)'}.

14. The representation of the total system is

s= {i, o, d, f}

i.e.

s={(m,n),(m),((cr)',(mr)',(k)',(sr)',(kc)',(d'),(f1,f2,f3,f4,f5,f6,f7,f8,f9,f10)}

IV. SYSTEM DESIGN

Least significantbit (LSB) insertion is a common, simple approach for embedding information in a cover image. The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message. Let us consider a cover image contains the following bit patterns:

Byte-1 Byte-2 Byte-3 Byte-4

00101101 00011100 11011100 10100110

Byte-5 Byte-6 Byte-7 Byte-8

11000100 00001100 11010010 10101101

Suppose we want to embed a number 200 in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information we need at least 8 bytes in cover file. We have taken 8 bytes in the cover file. Now we modify the LSB of each byte of the cover file by each of the bit of embed text 11001000.

As our eye is notvery sensitive so therefore after embedding a secret message in a cover file our eye may not be able to find the difference between the original message and the message after inserting

Some secret text or message on to it. To embed secret message we have to first skip 600 bytes from the last byte of the cover file. After that according to size of the secret message (say n bytes) we skip 8*n bytes. After that we start to insert the bits of the secret file into the cover file.

V. IMPLEMENTATION

The application would be built in MATLAB. We would compile and build the system project, create and sign the .exe file and install it into computer.

Fig.1. shows the interface where the User can encrypt secrete text message

Fig.2. shows the interface where the User can decrypt secrete text message

Fig.3. shows the interface where the User can get the decrypted secrete text message

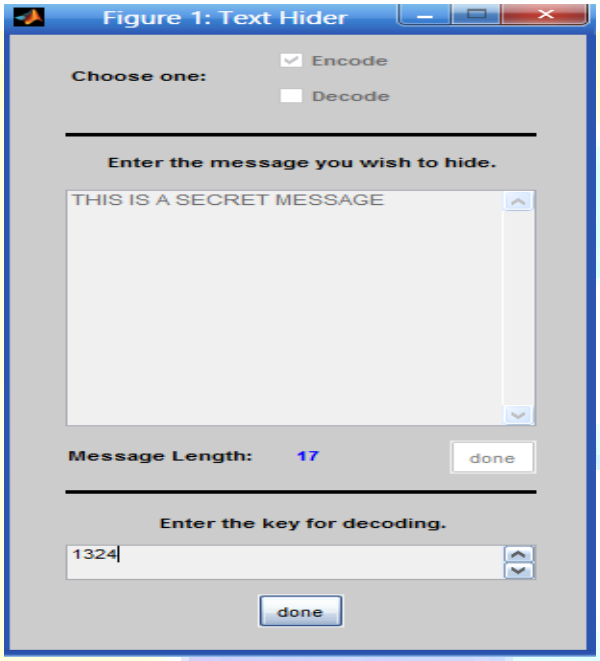


Fig 1. Encrypt Text

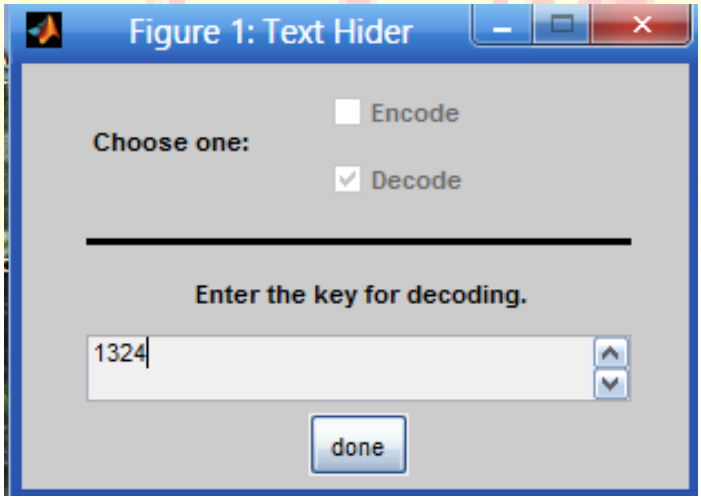


Fig 2. Decrypt Text

Fig 3. Decrypted Text

VI. RESULTS AND DISCUSSIONS

We have developed a system that has following functionality:

- The text or SM is taken by the user
- The cover file is selected by user which is to be used for encryption
- A secret Key is taken from the user which is mandatorily used at the decryption side
- During the text extraction the extrsaction algoritham is used to decrypt text after the key is matched.
- SM is then displayed on the reciver side

VIII. CONCLUSION

There exists some research on the development and validation of technological tools for driving monitoring. Some of them come under driver vigilance monitoring,and they focus on monitoring and preventing driver fatigue.In this paper we have extended the work of rash driving detection by proposing a scheme to monitor the driving patterns using the accelerometer and orientation sensors present in most of the smatphones today. We have used a pattern matching algorithm to match the values obtained from sensors at run time with the pre-stored test cases of rash driving data and generated an alert if patterns are matched. The alert generated is in the form

of a message, alarm and a call. As a part of the project, we have also provided driver with different speeds and distance values. involved in his journey viz. maximum speed, average speed, total distance travelled etc so that he could judge his driving style on a fair basis. This solution will negate the use of specialised hardware thus helping reduce cost and making implememtation faster and easier.

References

[1] Symmetric key cryptography using random key generator, A.Nath Vol. 2, No.3, March 2011 , S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244

[2] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, Page-392-397, 2010.

[3] Advanced steganographic approach for hiding encrypted secret message in LSB ,LSB+1,LSB+2 and LSB+3 bits in non standard cover files, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath , to be published in IJCA(USA),Vol 14-No.7, P-31-35, February 2011.

[4] Cryptography and Network , William Stallings , Prectice Hall of India

[5] Modified Version of Playfair Cipher using Linear Feedback Shift Register, P. Murali and Gandhidoss Senthilkumar, UCSNS International journal of Computer Science and Network Security, Vol8 No.12, Dec 2008.

[6] Jpeg20000 Standard for Image Compression Concepts algorithms and VLSI Architectures by Tinku Acharya and Ping-Sing Tsai, Wiley Interscience.

[7] Steganography and Seganalysis by Moerland, T , Leiden Institute of Advanced Computing Science.

[8] SSB-4 System of Steganography using bit 4 by J.M.Rodrigues Et. Al.

[9] An Overview of Image Steganography by T.Morkel, J.H.P. Eloff and M.S.Oliver.