ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

RMP ZR 1.0, an Efficient Algorithm to Stop Secret Communication through Steganography over Internet

[1]Er. Rakesh Kumar, [2]Pratik Kumar

Computer Science Researcher, Dept. of Computer Science & Engineering, Ranchi University, India[1]

B. Tech. Final Year, Dept. of Computer Science & Engineering, CIT, Ranchi University, India[2]

ABSTRACT: As we know, Social Networking Sites are being used in Terrorist Activities for secret communication by the Terrorists. That's why, it has become prime necessity of different countries like India, U.S.A, Russia etc. to find a solution to stop these secret communication. In this research paper, we have introduced a new and efficient technique that will stop secret communication over internet (or Social Networking Sites). In this research, we have used Steganography and Cryptography both. RMP ZR 1.0 will give full control to the Social Networking Sites over the transfer of Stegano Images. It may be proved to be very successful technique to make terrorists attempt failure.

KEYWORDS: RMP ZR 1.0, secret communication, Terrorist Activities, Steganography, Cryptography.

I. INTRODUCTION

RMP ZR 1.0 is an efficient technique which will meet the prime necessity of countries like India, U.S.A, Russia etc to stop secret communication over internet (or Social Networking Sites). The basic principles behind the development of RMP ZR 1.0 are the concepts of Steganography as well as Cryptography. If a sender *'A'* sends a hidden *message (or information)* behind an image through a Social Networking Site, *'Mbook'* to *'B'* then the receiver *'B'* will surely receive the image, though *'B'* cannot retrieve the original message as sent by *'A'*. The reason behind this is that RMP ZR 1.0 will be applied to the image just when the user clicks the upload button.

Cryptography Versus Steganography: Steganography[1] differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. The comparison and contrast between steganography and cryptography is illustrated from the following table[2]:

S. No.	*Context*	*Steganography*	*Cryptography*
1.	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2.	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3.	Result	Stego File	Cipher Text

DOI: 10.15680/IJIRCCE.2015. 0309092

4.	Type of Attack	Steganalysis: Analysis of a file with an objective of finding whether it is stego file or not.	Cryptanalysis

Table No. 1.1

II. INITIAL RESEARCH WORKS:

1. We have sent a .bmp image of size 20x20 through Gmail to a Gmail-id and then downloaded the image at the receiver’s end.
2. We have uploaded a bitmap image (.bmp), a .jpeg image, a .png image and a .gif image of size 20x20 at Facebook. After that we downloaded the image.
3. We have sent a .bmp image through Whatsapp and downloaded the image at the receiver image.

We compared the original image with the image we obtained after download as from the receiver’s end.

Conclusion 1: When we downloaded the image from Gmail we obtained .jpeg image instead of the .bmp image which was sent.

Conclusion 2: When we downloaded the image from Facebook we got .jpeg image instead of .bmp and .jpeg. As far as .png and .gif image are considered we got the .png and .gif respectively.

Conclusion 3: In case of WhatsApp we obtained the same result as we mentioned in Conclusion 2.

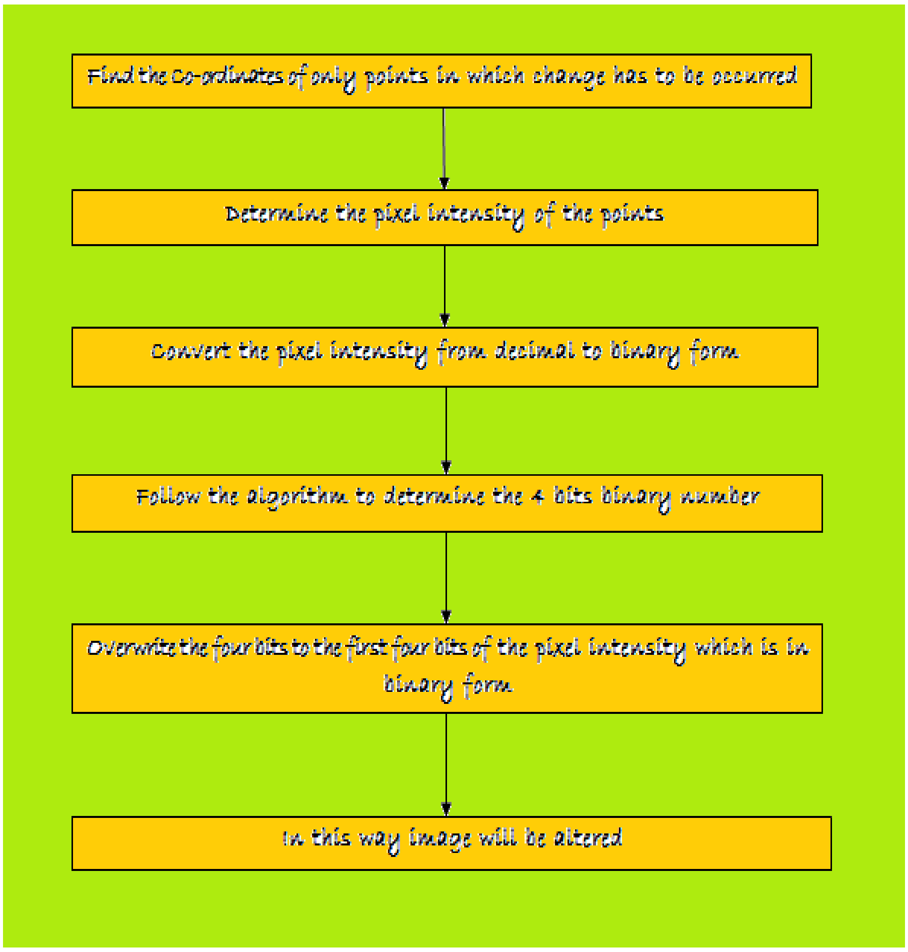
Final Conclusion of our Initial Research Work:

We conclude from the analysis that the image obtained after download will have the same extension as of the image which was sent by the sender. This conclusion is not valid for .bmp image. If we send a .bmp image it will be converted into .jpeg image (Due to compression) that means if a sender sends an image in .bmp format the sender will receive .jpeg image when he/she downloads the image.

III. PROPOSED ALGORITHM

Assumption: We are assuming all the images which are being transferred over a network, are the Stego images. That’s why to check this we will apply this Proposed Algorithm to all the images while they are being uploaded. For instance, suppose X, Y are the terrorists and X is trying to send some information hidden behind a career image to Y. For this when he just clicked the image button, this Algorithm will be applied to the image firstly then it will be uploaded to the network. In this case B will surely get the image but he will not be able to retrieve the original message as sent by A, because of modification.

DOI: 10.15680/IJIRCCE.2015. 0309092



Find the Co-ordinates of only points in which change has to be occurred

Determine the pixel intensity of the points

Convert the pixel intensity from decimal to binary form

Follow the algorithm to determine the 4 bits binary number

Overwrite the four bits to the first four bits of the pixel intensity which is in binary form

In this way image will be altered

Consider the taken image as Figure 1.

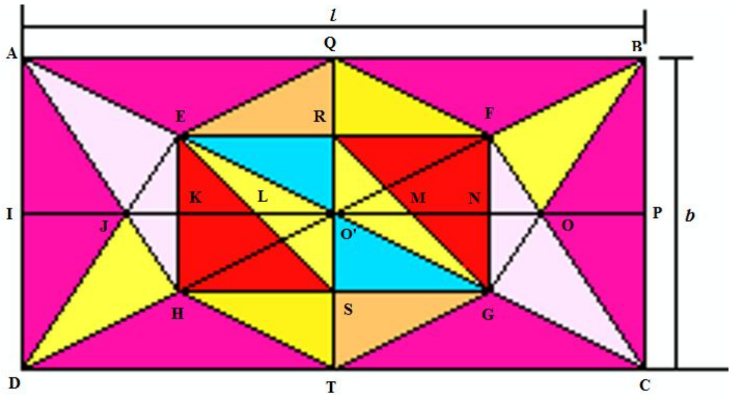


Figure 1

where *l* and *b* are the length and the breadth of the image (dimension of the image i.e. *l* x *b*)
In this research, we have used Steganography as well as Cryptography both. The reason behind this is that either Steganography or Cryptography alone is an efficient technique for secret communication over the internet (or Social Networking Sites). It is not safe enough to communicate secretly over an unsecured network using one of them alone.
Step 1: Find out the co-ordinates of point A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, O', P, Q, R, S, T as follows:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A ≡ (0, 0)	B ≡ (*l*, *b*)	C ≡ (*l*, *b*)	D ≡ (0, *b*)
E ≡ (*l*/4, *b*/4)	F ≡ (3*l*/4, *b*/4)	G ≡ (3*l*/4, 3*b*/4)	H≡(*l*/4,3*b*/4)
I ≡ (0, *b*/2)	J ≡ (*l*/6, *b*/2)	K ≡ (*l*/4, *b*/2)	L≡(3*l*/8,*b*/2)
M ≡ (5*l*/8, *b*/2)	N ≡ (3*l*/4, *b*/2)	O ≡ (5*l*/6, *b*/2)	O'≡(*l*/2,*b*/2)
P ≡ (*l*, *b*/2)	Q ≡ (*l*/2, 0)	R ≡ (*l*/2, *b*/4)	S≡(*l*/2,3*b*/4)
T ≡ (*l*/2, *b*)			

Step 2: Find out the pixel intensity of the points A, B, C, ……, R, S, T by using *Algorithm RZ 1.0*
Step 3: Convert the pixel intensity from decimal to binary form.
Step 4: Consider only the first eight bits of the pixel intensity (which is converted into binary form).
Step 5: Find X as

$$X = (Z + Pv)$$

where Z = first eight bits of the pixel intensity and
Pv = eight bits of position value in the binary form

Step 6: Find r1 as

$$r1 = rand() \% 255$$

Calculate $(key)_{10}$ using the following formulae:

$$(key)_{10} = \begin{cases} r1 + 100 & // \text{ if } r1 < 100 \\ \left(\frac{r1}{2}\right) + 50 & // \text{ if } r1 > 100 \end{cases}$$

Step 7: Find $(key)_2$ i.e. K_2 (say).
Step 8: Create message as follows:
M1 =

X	K_2'	X'	K_2	X'	K_2'	X	K_2
X	K_2'	X'	K_2	X'	K_2'	X	K_2
X	K_2	X'	K_2'	X'	K_2	X	K_2'
X	K_2	X'	K_2'	X'	K_2	X	K_2'

(Note: 1 block = 8 bits)
Where X, X', K_2 and K_2' all are of 8 bits.

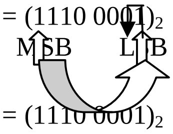
KEY =

B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8
B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}	B_{16}
B_{17}	B_{18}	B_{19}	B_{20}	B_{21}	B_{22}	B_{23}	B_{24}
B_{25}	B_{26}	B_{27}	B_{28}	B_{29}	B_{30}	B_{31}	B_{32}

$B_1 = K_2$;

Up to B_8 follow the following instruction Shift the MSB to the LSB position and shift the LSB to one bit towards left.
For instance, $K_2 = (11100001)_2$ hence,

$B_1 = (1110\ 0001)_2$



$B_1 = (1110\ 0001)_2$
$B_2 = (1100\ 0011)_2$
$B_3 = (1000\ 0111)_2$
And so on…
From B_9 to B_{16} follow the following procedure :
B_9 =

DOI: 10.15680/IJIRCCE.2015. 0309092

Bit 8	Bit 7	Bit 4	Bit 3	Bit 6	Bit 5	Bit 2	Bit 1

For instance, B9 = $(11001001)_2$ (From the above).
And so on..
Now Calculate as follows :

$B_{17} = B_1$ OR B_2; $B_{18} = B_1$ OR B_3 $B_{19} = B_1$ OR B_4; $B_{20} = B_2$ OR B_3
$B_{21} = B_2$ OR B_4; $B_{22} = B_3$ OR B_4 $B_{23} = B_5$ XOR B_6; $B_{24} = B_5$ XOR B_7
$B_{25} = B_5$ XOR B_8; $B_{26} = B_6$ XOR B_7 $B_{27} = B_6$ XOR B_8; $B_{28}=B_7$ XOR B_8
$B_{29} = B_9$ AND B_{10}; $B_{30} = B_{10}$ AND B_{12} $B_{31} = B_{13}$ AND B_{14}; $B_{32} = B_{15}$ AND B_{16}

Now we will perform XOR operation between M1 and KEY such that

Res = M1 XOR KEY

Res will be of 256 Bits.
Step 9: Apply MATLAB Code RZ 2.0, a Data Compression Technique and store it in RRes.
Step 10: Repeat Step 9 and overwrite the value in RRes until RRes is reduced to 4 bits.
Step 11: Overwrite these 4 bits to pixel intensity (in binary form) of the pints A, B, C, ……, S, T.

Algorithm RZ 1.0

Step 1: Open the image in MATLAB. For instance, consider the following statement:

a = imread(‘ D:\sti\N_Image1.bmp ’);

Here ‘a’ is a variable used in workplace; ‘N_Image1.bmp’ is an image which is stored in ‘sti’ folder in ‘D:\’ drive; and ‘imread’ is a MATLAB Command.
Step 2: Find out a_1, a_2, a_3 as follows:
a_1=double(i(:,:,1))
a_2=double(i(:,:,2))
a_3=double(i(:,:,3))
Step 3: Determine ‘x’ using the following mathematical statement:

$$x=a_1+a_2+a_3$$

MATLAB Code ***RZ 2.0*****:**

```
clc;
clear all;
close all;
sig=1:4;
Symbols=[1 2 3 4];
P=[0.1 0.3 0.4 0.2];
dict=huffmandict(Symbols,P);
temp=dict;
for i=1: length(temp)
temp {i,2}= num2str(temp{i,2});
end
disp(temp);
hcode= huffmanenco(sig,dict)
```

V. SCOPE AND FUTURE

The features of RMP ZR 1.0 can be enhanced in near future that may help to suppress *Terrorism*.

VI. CONCLUSION

This *Algorithm RMP ZR 1.0* is found to be very efficient and successful to stop secret communication over Internet or Social Networking Sites through image steganography. If RMP ZR 1.0 is used then no secret information of our Nation '*India*' can be sent to different countries by the spy placed in our countries. This is the reason why terrorism will be reduced up to much extent. RMP ZR 1.0 will give the control to '*The Indian Defense*' over the terrorist activities.

REFERENCES

1. T.Morkel, J.H.P. Eloff and M.S.Olivier. 'An Overview Of Image Steganography.' ,Information and Computer Science, University of Pretosia, in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.
2. Vijay kumar Sharma and Vishal srivastava. 'A Steganography Algorithm For Hiding Image In Image by Improved LSB Substitution By Minimize Detection.' ,Journal Of Theoretical and Applied Information Technology, Vol 36, No 1,ISSN: 1992-8645, Feb 2012.

BIOGRAPHY

He has done B. Tech in CSE from CIT, Ranchi in 2015. He has designed his own programming language namely RAKs. M. PLUS which will be better and faster than c++ in many respects. He is nominated for *Honorary Doctorate* for his successful research works at *I.N.O.U, Lucknow.* He gave his valuable contribution in the field of Information security. He also proposed a new methodology to find the steganographic signature of different steganography tools. He is currently working on 'Virus pot & Information security'. Image Processing, Cryptography, Information security and Data mining are his research areas of interest.

Pratik Kumar
He is a student of B. Tech in Computer Science and Engineering (Final year), CIT,Ranchi with a good Academic skills and have a keen interest towards the research works in the field of Computer Science. His research areas of interest includes Digital Image Processing, Wireless Sensor Network and Signal processing. He is a Co-author in the Original Research article published in International Journal Of Computer Science and Communication, entitled as "RAKS. M. PK 1.0 an efficient methodology to determine the Steganographic signature of Steganography tools".

DOI: 10.15680/IJIRCCE.2015. 0309092