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 Modern Approach for Data Transformation in Networks with New Methodology

A.Santhoshi, Dr.R.China Appala Naidu, E.Soumya, K.Meghana

Asst. Professor, Dept. of IT, St.Martin's Engineering College, Hyderabad, India

Professor, Dept. of CSE, St.Martin's Engineering College, Hyderabad, India

Asst. Professor, Dept. of IT, St.Martin's Engineering College, Hyderabad, India

M.Tech Student, VITS, Vishakapatnam, Tamil Nadu India

ABSRACT: Now a day's transfers the information from one place to another place over the internet is critical issue. So there are many techniques are available to protect the data while transfers the information from the hackers. In this paper we proposed new methodology which will used for encrypt the data at sender side and the receiver also decrypt the data with this methodology. The new methodology consists of key and image to secure the data from hackers. We tested this methodology, the methodology works properly and gives good results, with this methodology the data is transmitted securely and received without noise.

KEYWORDS: Hacker, encrypt, decrypt

I. INTRODUCTION

Now a day's using the internet for the communication has increased more. So security is also big issue for protecting the data from hackers, for these many of the cryptography techniques are used to protect such a kind of data. These techniques are like hash algorithm, symmetric, Asymmetric algorithms.

Cryptography is technique for securing the data. This system generally classify along three independent scopes:

1. Type of operations is used for transferring plain text to cipher text.
2. The number of keys is used.
3. The way in which the plain text is processed.

The main aim of using the cryptography is for Encryption and decryption of the data. The encryption is converting the plain text into cipher text [8][14][16] which is done at the sender side. The decryption is convert the cipher text into plain text, which is done at the receiver side.

Plain text:

Plain text is an original message or data.

The encryption algorithm does several transformations on this plain text. And the secret key also used as the input to encryption algorithm.

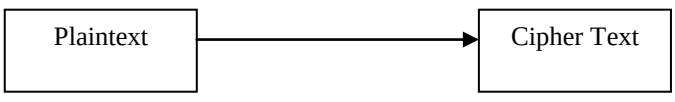

Fig.1.plain text to cipher text

Cipher text:

Cipher text is scrambled message produced as output.

At the receiver side, decryption algorithm is used to decrypt the cipher text into plain text by using secret key. This decryption process runs reversely for the encryption algorithm.

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

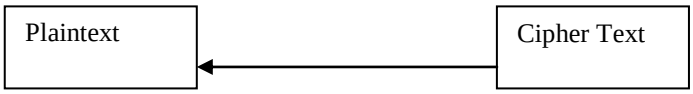

Fig.2.Cipher text to plain text

Steganography: This word steganography comes from the Greek words steganos means "covered, protected" and graphy means writing [7][13]. Steganography is hiding the data, file, message, image or video within another file, message, image or video. This steganography means concealing the message itself by covering it with something else.
Now a day's any form of the information like text, image, audio & video can be digitized and it is possible to insert secret binary information into the data during digitization process.
Steganography has many applications and useful objectives; those are undetectability, strength, confrontation to different methods of image processing, compression [3][9][11]. It needs two kinds of data in which one is "the cover", and second is "the data to be hidden".

Cover: The cover is an image which we will hide the data. Selecting the required cover is very significant; it determines the effectiveness of steganographic technique. If the image has less number of colors for embedding the data, it is uncomplicated to detect data. For example the cover image contains only one color, which we will hide data into that image. So after embedding the data it into there will be two colors[2][5][15]. These colors are very similar, but not the same. This is simple to find the data which we hide in the image. Upon this an image has many colors, after embedding also has many colors and for each color it has different numbers. So it is intricate to find the data from such a kind of image.

Text Cover: The cover of secret data can be text
Image Cover: the secret data can be covered with image. Digital images contains the pixels, in this each pixel uses the 24bits [1][4]. Each byte having colors (red, green, blue). We can hide the binary information in the image by keeping (or) changing the least significant bit.
Other Covers: The message (or) data can also be covered under the audio & video. Today audio and video are compressed, so the secret data can be embedded during or before the compression.

Data: Bit by bit embed into image cover which should be serializable. The data is no longer than cover image, but it may be equal. But the cover has so many colors, so that have many pixels also. That's why compare the data size with cover image pixel size[5][10]. Whatever the data wants to embed into cover image that data is in binary format.
The main advantage of steganography is that the secret message is sent.

Hacking: The Hacking is any technical activity (effort) to manipulate the normal behavior of network connecting.
The Hackers is a person who attacks the network and hack the information.
This Hacking is done with other network programming and this kind of special programs are generally using to manipulate the data, Which is passing through the network[6,12]. In present day, huge amount of information is using in business and exchanging the data. The Hackers are very intelligent persons who theft the important information from the data.
The Hackers attacks on the network when the sender starts transferring the information (or) data to receiver.
In[1] the binary series ,the lowest bit is consider as least significant bit, and which is right most bit of the string. For example, in binary series 10010101, the least significant bit is right most bit 1. This method is also used to find the even or odd. Sometimes the right most bits are changed rapidly. For example binary 5 is 00000101, 6 is 00000110, so here least significant bits will change 101 to 110.

II. RELATED WORK

In [1][6],they proposed a steganography, to hide a message in a cover, such that there would not be apprehensive. Here least significant bit – 2 concepts was applied for embedding as a text. Digital Image which are stored in either 24-bit (true color images) or 8-bit per pixel files [3][8], based on the pixel size and number of colours the data to be hidden.

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

In [16], authors are used a method to transfer the data from user1 to user2. According to their [4][16]methods ,encrypt the given message and transfer the cipher text along the key to receiver.

III.PROPOSED METHOD

In this proposed system, two exponents a and b are uses, where a is public and b is private. Let P is a plain text, C is cipher text. Suppose sender wants to send a message or text to receiver, it converts into cipher text $C=P^a \mod m$ is use to create cipher text C from the plain text.
And at the receiver end uses $P=C^b \mod m$ to receive the plain text whatever transfer by the sender. Both the sender and receiver must know the values of m, a and only the receiver knows the value of b. In this algorithm the public key is {a, m} and private key is {b, m}.
For this algorithm, these are the main requirements:
a)Finding the values of a,b,m so that $P^{ab} \mod m=P$ for all P<m.
b) It is easy to calculate P^a and C^b for all P<m
c) It Is infeasible to determine b given a and m.
Here m is calculated with two prime numbers, which is product of those two prime numbers.
Let's consider i and j are two prime numbers, m=i×j which is modulus for the encryption and decryption.
If I and j are the large prime numbers then m is very complex.
Then find the ϕ(m), which is positive integer less than m and relatively prime to m.
Then select an integer a that is relatively prime to ϕ(m).Then find the value of the b as multiplicative inverse of a, modulo ϕ(m).

Key Generation:

Select i , j	i,j are prime numbers i≠j
Calculate m=i×j	
Calculate ϕ(m)=(i-1)(j-1)	
Select integer a	gcd(ϕ(m),a)=1; 1<a<ϕ(m)
Calculate b	ba mod ϕ(m)=1
Public key	{a,m}
Private key	{b,m}

In this algorithm, encryption and decryption is done by generating the keys.

Suppose there are two users A and B. The sender is user A, receiver is User B. the user wants to send the data to user B. The actual data is plain text that is encrypted with key 'a'. The output of plain text is cipher text, which is transfer to receiver side 'B'. Not only the cipher text, has the key also transferred to receiver side. This key is used to decrypt the data at receiver side. So this key is an important to convert the cipher text to plain text which is send by the User A. But there are many chances to attack on this transmission data. To secure the key here we propose the method is embedding the key in image. The key is hidden in an image by using steganography technique. The cover image, true color supports 24-bit for RGB colors. This is the clear and strong graphical image in RGB color space, so that very large number of colors and shades can be displayed in an image.

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

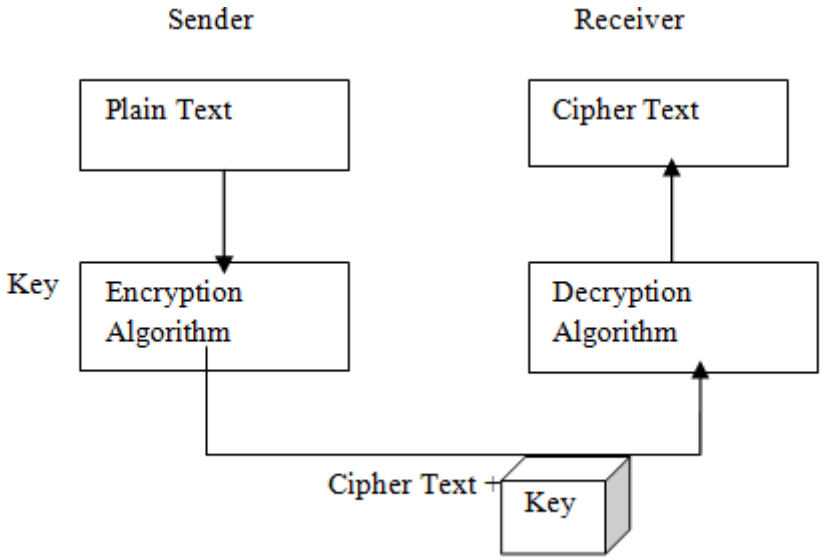

Fig.3. Key in secured image

In this method the key is embed at the least significant bit of image pixel.
The following steps illustrate how this method is used to hidden the secret key in cover image.
Step 1: Change the hidden data from decimal to binary

[Key data in decimal] ——— to ———▶ [Binary]

Example: Key is 78

[78] ———▶ [01001110]

Step 2: Let's consider 24-bit image pixel

01111011	10010000	00111101
10000101	10000011	01001100
10011001	01111000	10101111

Step 3: Replace the least significant bit by on bit of the data which is to be hidden

First byte of the actual data from the image pixel

0	1	1	1	1	0	1	1

First bit of the key to be hidden:

0

Replace the least significant bit:

0	1	1	1	1	0	1	**1**

0

0	1	1	1	1	0	1	**0**

Step 4: Repeat the same process for all the bit of the key

Then the embedded pixels are:

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

01111010 10010000 00111101
10000100 10000010 01001101
10011001 01111001 10101110

Embedding the data (binary) into image(pixel) Algorithm :

Step 1 : Message of binary, Bit={$B_0, B_1, B_2 \ldots\ldots\ldots B_{65535}$}

Step 2: Pixel of the cover image, Pixel : {$X_0, X_1, X_2 \ldots\ldots X_{65535}$ }

Step 3: LSB-1 of the cover image, LSB1={$L_0, L_1 \ldots\ldots\ldots L_{65535}$}

Step 4 : For n=0 to message length do

```
{
 If  Bi = Li  then
     Do nothing
  Else
     {
       If  Bi = 1 AND  Mi = 0 then
       {
        Bi = Mi
        X (n)+ =1;
}
       If  Bi = 0 AND  Mi = 1 then
       {
        Bi = Mi
        X (n)+ =1;
            }
}
}
```

IV.CONCLUSION

The data is very securely transferred from sender to receiver, in this paper our proposed methodology combines the key with an image, the same was received by the receiver and decrypts the same and fetch the key from an image. The key is embedding into image based on the least significant bit, which is very clear and effective method. This methodology works very well, without any noise and any problem the data is transmitted and received by the receiver.

REFERENCES

[1]. A. E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD, " A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", Research Journal Specific Education, Issue No. 21,pp 8-14. April. 2011
[2]. Alain C. Brainos II, "A Study Of Steganography And The Art Of Hiding Information", East Carolina University, pp.3-4
[3]. Neil F. Johnson Sushil Jajodia ," Exploring Steganography: Seeing the Unseen ",0018-9162/98/ © IEEE ,pp. 3-4, 1998
[4] . Mei-Yi, W., Yu-Kun, H. , Jia-Hong, L," An Iterative Method of Palette-Based Image Steganography", Journal of Patern Recognition Letters, Vol (25),2004
[5]. Alain, C. Brainos (), "A Study Of Steganography And The Art Of Hiding Information", East Carolina University.
[6]. Desoky, A,"A novel Noiseless Steganography Paradigm", Ph.D, Department of Computer Science and Electrical Engineering, Faculty of the Graduate School, University of Maryland, Baltimore County,2009
[7]. Christopher. T,"Compression Aided feature Basedsteganalysis of Perturbed Quantization Steganography in Jpeg image" ,Ms.C s, Department of Science in Electrical and Computer Engineering,
University of Delaware,2009
[8]. Xiang-yang, L. , Dao-shun,W., Ping, W., Fen-lin, L," A review on Blind Detection for Image Steganography, Journal of Signal Processing, Vol(88),Issue(9),2008.
[9]. Samer, A,"A New Algorithm for Hiding Gray Images using Blocks, Information , Security Journal, The Hashemite University, Jordan, Volume (15), Issue (6),2006
[10]. Gerad, G," An Investigation of Scalable Vector Graphics as Cover Medium for Steganography, Ms.C, faculty of college of arts and science, American University,2006
[11]. Kaushal M. Solanki, Multimedia Data Hiding:From Fundamental Issues
to Practical Techniques, Ph.D, Electrical and Computer Engineering,university of california, Santa Barbara,2005
[12]. Sanjeev, M.,et.al ," Customized and Secure Image Steganography, Journal of Signal Processing" , Vol(1), Issue (1),2008
[13]. Hengfu, Y., Xingming S., Guang S, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal of radio engineering, VOL. (18), NO. (4),2009

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

[14]. Lee, L, LSB Steganography :Information Within Information, Journal of Computer Science,Vol (265), No (5),2004
[15]. Chi-Kwong,C., Cheng, L, "Hiding data in images by simple LSB substitution", Journal 0f Pattern Recognition, Vol (37),2004
[16]. https://en.wikipedia.org/wiki/Cryptography

BIOGRAPHY

1**. A.Santhoshi** completed her M.Tech from JNTU Hyderabad and she has 8 years of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is Network Security, Security in Big data, Dataware Housing.

2. **Dr.R.Ch.A.Naidu** completed his M.Tech, Ph.D from University of Mysore, Mysore and Andhra University, Vishakhapatnam respectively. He has more than 13 years of teaching experience. He is presently working in CSE Dept as a Professor in St Martin's Engineering College, Hyderabad. He has life membership in professional bodies like ISTE, CSI. His area of interest is Network security, Computer networks, Digital Image processing, Data base management systems .He has life membership in professional bodies like ISTE, CSI.

3. **E.Soumya**, Completed her M.Tech from Kakatiya University, Warangal and she has 7 years of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is Network Security, Computer networks, Dataware Housing

4. **K.Meghana** completed her B.Tech from JNTU Kakinada in the year of 2014. Now she is doing her M.Tech in VIT, Vishakapatnam in CSE department. She published 3 papers in international journal. Her interested areas are Network security, Data management systems, Automata and Compiler design.