A Review Paper on Steganography

Kirti[1], Kamaldeep Joshi[2]
Department of Computer Science and Engineering,
University Institute of Engineering and Technology,
Rohtak, India
[1]kirtikangra98@gmail.com
[2] kamalmintwal@gmial.com

***Abstract*—Steganograhy sends message by concealing it so that intruder can't detect the presence of message. It is an art of hiding information in digital media. It ensures that communication between two parties remains secure, their communication should be undetectable. As this era is of internet, secure communication is very difficult to achieve. So, to achieve this in this paper an overview of steganography and various techniques are discussed. In modern era various new techniques came in existence. There are two types of the steganography one spatial and other is frequency domain. This paper concerned about spatial domain and some part of frequency is also explained.**

***Keywords*—Steganography, LBS, FMM, Interpolation, Parity check, Logic gates, Frequency domain, DFT, DCT, DWT.**

I. STEGANOGRAPHY

Steganography is an art of hiding data. The word steganography combines the Ancient Greek words stegano that means "covered, concealed, or protected" and graphy means "writing"[1]. Steganography and cryptography both are used for the secure communication but the way of working is different where cryptography encode the message where as steganography hides the presence of the message. It can hide the information in image, audio, video in all the digital media [1,2].Before steganography cryptography used. Cryptography is also considered for hiding data for many years but some time it fails to provide secure communication. But now these days steganography is used to communicate [2].

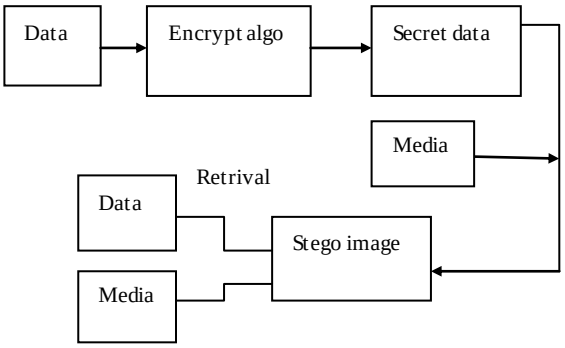

Fig. 1 Block Diagram of Steganography

Steganography does not means to revise the structure of message however it hides the secret message inside a cover object. The embedding of secret data depends on the size of cover object. Steganography consists of two terms that are message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it [3]. Steganalysis is a process of crack the cover object in order to get the secret data. In general terms, it is known as unauthorized access of data during transmission.

II. TYPES OF STEGANOGRAPHY

A. Text based steganography

In this method secret message is to hide in text file. It can hide message by various ways:-

- Format Based Method
- Random and Statistical Method
- Linguistics Method

B. Audio steganography

In this message is to hide in audio file .In this message is embed in MP3, WAV, AU sound formats. It can hide message by various ways:-

- Low Bit Encoding
- Phase Coding
- Spread Spectrum

C. Image steganography

In this message is to hide in image. It can be classified in different categories. These are:-

- Spatial Domain
- Frequency Domain
- Adaptive

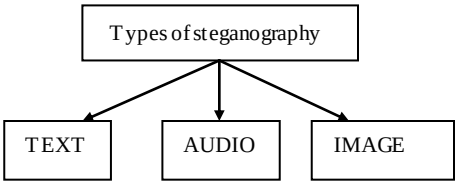

Fig. 2 Types of steganography

III. IMAGE STEGANOGRAPHY

In this image is used as the cover object to hide the data. Pixels are used to hide data. Image after hiding data is known as Stego image. In digital era image is used as cover media as it contain number of pixels to hide data in it.

© 2016 IJAIR. All Rights Reserved

IV. CLASSIFICATION OF IMAGE STEGANOGRAPHY

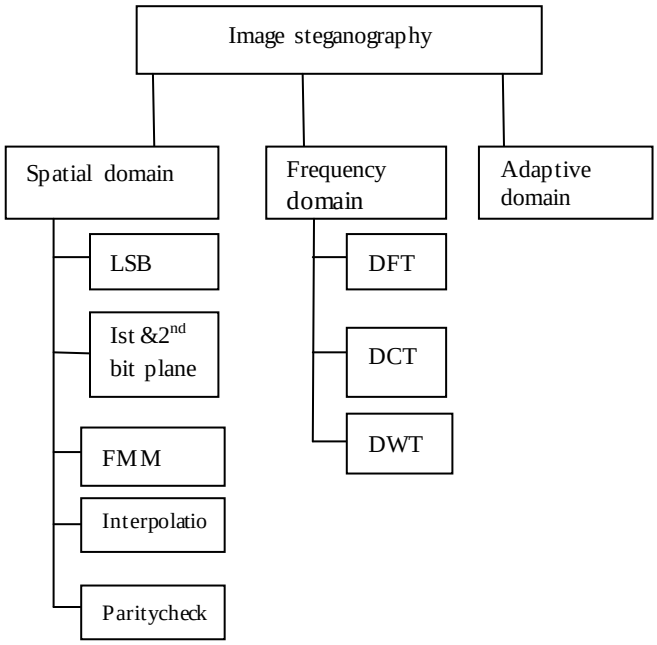

Fig.3 Types of image steganography

A. Spatial Domain

In spatial domain, cover image and secret data hide by using LSB and level encoding. First, the cover image is split into bit planes and then LSB of bit planes replaced with secret data. LSB is most common used steganographic technique.

Some common techniques which are used to conceal the message in image.

1) Least Significant Bit Method:- In this method of steganography, the least significant bits of the cover media are used to conceal the message[10,11]. This is the simplest method.In this replacement of the last bit of each of the data values to reflect the message that needs to be hides.

Let just take an eg :-suppose alphabet "M" is to hide in image. Value of pixels (0-255) are known. First convert them in binary. Suppose values of pixels are following-

110 - 01101110 120 - 01111000
150 - 10010110 240 - 11111010
180 - 10110100 190 -10111110
160 - 10100000 250 - 11111010

ASCII value of "M"= 109 and in binary = 01101101

Now check the last pixel value if it is same as message bit than won't need to change the value.

If no, than try to convert it in message bit by adding or subtracting '1' and send to the receiver.

After applying the algorithm pixel values become-

110-> 01101111-> here add 1
120-> 01111000-> don't need to the value of pixel as value is same message bit

150-> 10010111-> by adding 1

Remaining values are->

11111011 10110100 10111111 10100001 11111010

At receiver end or retrieval of message it checks the last pixel value of image.

Advantages:-

- Easy to implement.
- Invisible to human eye

Disadvantages:-

- Message can be easily retrieved by intruder.
- Message can be easily modified.

2) Message hiding in 1st and 2nd bit plane:- This method overcomes the limitations of L.S.B. insertion method. This algorithm hides data on 1st and 2nd bit of lsb. According to this algorithm the last two bit of lsb are checked [12]. 1st and 2nd bit of location means value of pixel are checked and try to transform the value of last bit of location same as message bit by adding or subtracting '1'.Ignore the boundary values(00000000 - 11111111) because the change may be +2 or -2 in pixel values.

Now let just take an e.g. suppose alphabet "M" is to hide in image. Values of pixels (0-255) are known. First convert them in binary. Suppose values of pixels are following-

110 - 01101110 120 - 01111000
150 - 10010110 240 - 11111010
180 - 10110100 190 - 10111110
160 - 10100000 250 - 11111010

ASCII value of "M"= 109 and in binary = 01101101

Now check the last two pixel value Are they same as the message? If yes than won't need to change the value of pixel . if no than try to convert it in message bit and send to the receiver.

After applying the algorithm pixel values become-

110-> 0110111-> here we add 1(1 time)

Check last 2 pixel values they are same as the first message bit. Now same process is applied to remaining pixel values.

120->01111000-> Don't need to the value of pixel as value is same message bit.

150-> 10010111-> here add 1(1 times)

Remaining values are ->

11111011 10110100 10111111 10100011 11111000

the whole process is insertion of message bit in pixel.

At receiver end or retrieval of message it check the last two pixel value of image if they are same than they consider as the message bit else ignored. This is simply the retrieval algorithm. When pixel value after adding or subtracting exceeds from 2 than we ignore that location.

Advantages:-

- Simple, Easy to implement.

Disadvantages:-

- Intruder can retrieve the message if any clue is captured.

3) Interpolation:- As every pixel in the image is correlated. In this method data is to hide in between the pixels .As range

© 2016 IJAIR. All Rights Reserved

of the pixels lie between 0-255.In this using some method suppose taking the mean of two nearby pixel and hide the data at resultant pixel. In the method more data can be hide with respect to any other method as data can be hide at other then middle pixels.
For eg:- Two pixels like 120-130, using mean so the resultant pixel will become 125 and data will hide on that pixel. Using the same method at the other end ,data can be easily retrieved.

Advantage:-

- More data can be stored as data is hidden at the intermediate pixel.

4) Five Modulus Method:- This is an effective method of steganography. In this method image is divided m*m blocks. So as the name suggests image is divided in 5*5. As the value of pixel is lie between 0-255 [13]. In this method value of each pixel should be divisible by the 5.
Following algorithm is used:-
If pixel mod 5=4
Pixel=pixel+1
Else if pixel mod 5=3
Pixel=pixel+2
Else if pixel mod 5=2
Pixel=pixel-2
Else if pixel mod 5=1
Pixel=pixel-1
Using this algorithm message can hide in the image .In this one pixel is selected in which one alphabet of message have to hide and the remaining pixels are divisible by 5 except that pixel.The process is repeated until the whole message will not hide.At the receiver end using this formula,data is retrieved

Alphabet value= (position+(remainder-1)* m^2)+(starting add-1)

For eg:- Value is 117, which is not exactly divisible by 5 so the alphabet is hidden here. By using above formula suppose position is 9. Now according to formula (9+ (2-1) 5^2)+(31-1)=65 and we know 65 is ASCII value of 'a' .So the alphabet hidden here is "a".

5) Parity checker:- In this method using parity data is to hide [14]. If even parity, than insert 1 at that pixel if odd than 0 .
For eg:-

110 - 01101110	120 - 01111000
150 - 10010110	240 - 11111010
180 - 10110100	190 - 10111110
160 - 10100000	250 - 11111010

ASCII value of "M"= 109 and in binary = 01101101
Now to check the parity count the no of 1's are they even or odd.
At 01101110-> no of 1's are odd but need to hide 1 so add 1 and transform this in even parity .Same process is applied to other pixels also.At the receiver end by counting no of 1's , hidden message will retrieve.
Advantage:-

- Least change in the pixel value because only parity has to set according to the data that is to be hide.

These are some methods which are used for the steganography to hide data .

B. Frequency Domain

In frequency domain, secret data is hide in noteable areas of covered image,which makes data revive to attacks such as compression, cropping or image processing methods. This method is also known as Transformation domain. In this technique image processing is done according to the frequency [16,17,18].Data is spread across the whole image so that it provides better protection against the signal processing. This provides an intensify security level to steganography method and lead to the development of algorithms.
Various methods are used for the transformation:-

- Discrete Frequency transformation technique
- Discrete Cosine transformation technique
- Discrete Wavelet transformation technique

1) Discrete Frequency Transformation (DFT):- DFT helps to get the frequency component for each pixel value. It produces complex number, which may be displayed either with the real or imaginary part or with magnitude or phase.. It is applied on source image to convert from spatial domain to frequency domain. Each pixel (8 bits) in spatial domain is transformed into two parts one part is real and another is imaginary part. The authenticating bits are inserted in real part.

2) Discrete Cosine Transformation (DCT):- DCT is a function which maps the input signal or image from spatial domain to frequency domain. DCT transforms the input into a linear combination of weighted basis functions. If DCT is applied twice then one dimension DCT become two dimensional DCT. Some basis functions are used for transformation. These basis functions are input for the frequency component [19]. when DCT is applied on the cover image weight matrix is produced which show how much the basis function should be present in cover image .For most images, much of the signal energy lies at low frequencies, which appear in the upper-left corner of the DCT. The lower-right values represent higher frequencies, and are often small small enough to be neglected with little visible distortion [19].The definition of the two-dimensional DCT for an input M x N image.

3)Discrete Wavelet Transformation (DWT):- DWT is a mathematical tool for systematically decomposing an image. It is useful for processing of moving signals. Small waves are used for the transformations which are known as wavelets, of different frequency and for limited time period. It provides both frequency and spatial description of an image. Mother wavelets are used for the rendering and enlarge the small wavelet. When transformation is performed on 2-D images,

© 2016 IJAIR. All Rights Reserved

then the image is process by 2-D filters in both dimensions. They decompose the input image into four parts. These parts are non-intersecting or multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 shows the coarse-scale Discrete Wavelet Transform (DWT) coefficients and remaining sub-bands as LH1, HL1 and HH1 indicate fine-scale of DWT coefficients. More coarser scale of wavelet coefficients are produced by using the DWT up to N level of it. Because of its great spatial-frequency localization attribute, the DWT is very appropriate to recognize the region in the cover image where we can hide a secret message effectively. Usually most of the image energy is stored at lower frequency, so steganography in these sub-bands may decrease the quality of image. However, embedding in low frequency sub-bands could increase robustness. In contrast, the high frequency sub-bands represents the edges and textures of an image. Usually people do not notice slight changes, so high frequency sub bands is more suitable for embedding without being notice by the human eye.

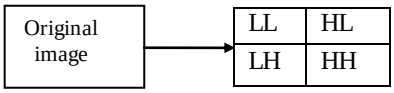

Fig.4 DWT

C. Adaptive Domain

This steganography method is a special case of two methods: spatial domain and transform domain. It is also known as "Statistics Aware Embedding" and "Masking". Global proper--ties of images are used before embedding secret data in factor of DCT or DWT. The statistics will decide where changes can be made.It makes random selection of adaptive pixel depending on the cover image and the selection of pixels in a block with large local standard deviation. It avoids the same colour areas. This behavior makes it seek image with with large local standard deviation. It avoids the same colour areas. This behavior makes it seek image with existing or deliberately added noise and images that demonstrate colour complexity.

V. New Emergence Methods

Digital logics are also used in steganography. Image is selected on the basis of digital logic.So that the embedded information would secure and no detectable change in image [20].

Three methods are proposed:-

- Logic Gate Method
- Shift Operator Method
- Combined Method

1) Logic Gate:- AND,OR,NOT etc are logic gates that used to derive the information matrix based on image matrix.

Insertion Method:- The message metrics and the image metrics are read in row major order so that no two columns of matrices have same value. Logic gates are used to get the information matrix from image matrix.

Some op codes are used for the logic operation:-

Logic Operation	**'Op' Op-Code**
AND	00
OR	01
XOR	10
NOT	11

These op-codes are used to generate the information matrix. The information matrix in image is in form of 'op-code, row address , row address'.

Suppose a 256*256 image and the information is of 1Kb. We can write this in information in matrix of 4 * 256, so that number of columns is equal in both image and information matrix. Suppose for the first row of the information matrix is formed by ANDing the 7^{th} and the 13^{th} position of image matrix. Then hidden data for first row of information matrix will be '0000000111000011101'.In this first two digits are the AND op-code and remaining bits are the address of image matrix. Some rules are also given if the desired image is not found to hide the information.

If the desired size of hidden information matrix is achieved after appending recursion, Master Bit Pattern is formed. By applying the recursive method size of the information matrix is of preferred size. The obtained MBP should be secured if any bit change then the retrieval of the information become difficult. Hence obtained bit pattern is coded using Turbo Code.

At the extraction end by using agreed addresses and turbo code is decoded to find the MBP. MBP is then decoded by decoder by applying the recursion operation.

2) Shift Operator Method:- This method is used when data need to be serially shifted. If the data is left shift than it is known as shift left operation and for right it is known as shift right operation.

Three types of operation are performed:-

1) Logical
2) Circular
3) Arithmetic

In logical operation shift left or right operations are performed.

In circular shift data is shifted from one end to another end . The data can be left or right circular shift.

In arithmetic operation singed binary bit is shift in left or right direction.

The message matrix and image matrix is read in row major order so that no two column of matrices have same value.

Some op codes are used for the shift operation:-

© 2016 IJAIR. All Rights Reserved

Shift Operation	'Op' Op-Code
SHL	00
SHR	01
CIL	10
CIR	11

In this method, rows of image matrix are shifted to form the rows of information matrix. Then hidden data in image is in form of, each row of information matrix will be op-code, row address, and numbers of shifts.
Suppose a 256*256 image and the information is of 1Kb and we perform 15 bit shift operation (circular left) on the 32th row address to form the any address of the information matrix. Then embedding for that information row will be 100010000000001111. In this first two digits are the shift operation op-code and next 8 bits are the address of image matrix and 8 bits are the no. of bits shift .This also work in same manner as the logic operator does.

*3) Combined Method:-*This method is combination of the previous two methods. In this method either logic operator or circular shift operators can be use. Op-codes are used :-

Operation	'Op' Op-Code
OR Gate	000
AND Gate	001
XOR Gate	010
NOT Gate	011
SHL	100
SHR	101
CIL	110
CIR	111

The cost of using this scheme is one extra bit in Op-code to accommodate more operations on image matrix. This scheme can also be applied in conjunction with turbo encoding and turbo decoding as used in Logic Gate Method

V. PERFORMANCE MEASUREMENT PARAMETERS

1) PSNR:- The Peak signal to noise ratio (PSNR) is ratio to determine the image quality of image .It is ratio between possible power and distorted noise that affect the image. If PSNR value is larger than image quality is higher. If value is less than shows more distortion between stego image and cover image.

2) MSE:- Means mean square error Given a noise free $m \times n$ monochrome image I and its noisy approximation K.

VI. APPLICATIONS

1) Secret communication can be established by means of hiding secret information with in digital media covers to hide presence of communication.

2) Secure storage means utilizing the cover digital media as secure storage for some sensitive information.

3) Covert communication for some organizations or people might be vital to keep their data safe against unauthorized people.

4) Copyright protection helps to protect dedicated resources to production of intellectual producers.

VII. CONCLUSION

In the past few years Steganography is interesting topic to make communication more secure. This paper gives an overview about Steganography and its techniques. All techniques of Steganography satisfy all the four properties (robustness, Imperceptibility, embeddingcapacity, payload capacity).In this paper some main methods of spatial domain have seen. LSB is the first method which was introduced but in this method static attacks are possible. So other methods were introduced. It depends on the user which method user chooses. Frequency domain a complex technique but this provides more security than spatial domain. This paper provides an overview, how steganography helps in secure communication.

REFERENCES

[1]"Maheswari,S.U., Hemanth,D.J." Differentmethodologyforimage steganography-based data hiding: Review paper Department of ECE, Karunya University, Coimbatore, India Volume 7, Issue 4-5, 2015
[2]"B.Saha , S.Sharma "Steganographic techniques of data hiding using digital images , Institute for Systems Studies and Analyses ,Volume 62, Issue 1, January 2012
[3]"Shaveta Mahajan, Arpinder Singh" A Review of Methods and Approach for Secure Stegnography , Volume 2, Issue 10, October 2012.
[4]"C.P.Sumathi, T.Santanam and G.Umamaheswari" A Study of Various Steganographic Techniques Used for Information Hiding Vol.4, No.6, December 2013.
[5]"Jagvinder Kaur and Sanjeev Kumar", Study and Analysis of Various Image Steganography Techniques, IJCST Vol. 2, Issue 3, September 2011.
[6]"Rakhi ,Suresh Gawande", A Review on steganography methods ,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013
[7]"James C. Judge" Steganography: Past, Present, Future GSEC Version 1.2f.
[8]"Jasleen Kour, Deepankar Verma" Steganography Techniques –A Review Paper, Volume-3, Issue-5 May 2014.
[9]"Arvind Kumar and KM. Pooja" , Steganography- a data hiding technique, international journal of computer applications (0975 – 8887) volume 9– no.7, November 2010
[10]"Chi-Kwong Chang, L.M. Cheng", Hiding data in images by simple LSB substitution Department of Computer Engineering and

© 2016 IJAIR. All Rights Reserved

Information Technology, City University of Hong Kong , Hong Kong , Received 17 May 2002
[11]"Rajkumar Yadav, (2011)" A Novel Approach For Image Stegano-graphy In Spatial Domain Using Last Two Bits of Pixel Values, International Journal Of Security, Vol.5 Iss.2 pp.51 61 .

[12]"Parvinder, Sudhir Batra and H.R Sharma", Evaluating the Performance of Message hidden in 1st and 2nd Bit Plane,W SLAS Transaction on Information Science and Technology. vol. 2, No. 89,Aug.2005.
[13]"Firas A. Jassim , Hind E. Qassim" five modulus method for image Compression. Vol.3 No.5, October 2012.
[14]"Rajkumar, Rahul Rishi, Sudhir Batra" A New Steganography Method For Grey Level Images Using Parity Checker, International Journal Computer Applications, Volume-11, May2010.
[15]"Sandeep Singh, Aman Singh" A Review on the Various Recent Steganography Techniques, IJCSN International Journal of Computer Science and Network, Volume 2,
Issue 6 December 2013.
[16]"N.Provos., P.Honeyman",Hide and Seek an introduction to Steganography, IEEE Security and Privacy 1(3),2004.
[17]"Arazoo Dahiya, Vandana", A Review on image Steganography using Frequency Domain, International Journal for Scintiffic Research & Development Vol.2,issue 02,2014
[18]"Dr. Mahesh Kumar,Munesh Yadav",Image steganography using frequency domain, International Journal for Scintiffic Research & Technology Research vol.3,issue9,2014
[19]"A. A. Al-Saffar ", Proposed Steganography Method Based on DCT Coefficients, ibn al- haitham j. For pure & appl. Sci. Vol. 24 (3) 2011.
[20]"Parvinder singh, Sudhir batra, HR Sharma" Steganographic Methods Based on Digital Logic 6th WSEAS International Conference on signalprocessing, Dallas, Texas, USA,
March 2007.

© 2016 IJAIR. All Rights Reserved