International Journal of Current Research in Multidisciplinary (IJCRM) *ISSN: 2456-0979*
Vol. 9, No. 8, (September'24), pp. 06-09

A BRIEF SURVEY OF VARIOUS STEGANOGRAPHIC TECHNIQUES

Shivani Sharma[1], Jasvinder Kaur[2]
[1]*Research Scholar, Dept. of Computer Science, PDMUniversity,Haryana, India*
[2] *Assistant Professor, Dept. of Computer Science, PDM University, Haryana, India*

ABSTRACT: Secure communication has become an important part to establish a connection so we make sure that no intruder is able to access our data hence steganography came into role.Steganography is defined as the "covered writing" or "hidden writing" which helps to make the data invisible for the intruder. The privacy of our data is managed so that no malicious attacker is able to access the data. This can be achieved by so many technologies, as we know that new technologies are emerging day by day so it is easy for us to achieve it. So, in this paperwe are going to study few steganography techniques for the data privacy and security.

KEYWORDS: *Steganography, LSB, cryptography, MSB, DWT, DCT.*

INTRODUCTION

Security has become oneof the most challenging aspect in our society. Security is required in each and every part of the communication. For communication, the sender and receiver play an important role and transfer the data which is very easy to access, so in order to secure the data cryptography was developed. Here the sender utilizes encryption algorithm for encoding the dataand recipient utilizes decoding algorithm for unscrambling the data.But as time goes it became very easy for intruders to access the dataas they can break the code and access the data[1]. So, to overcome this, steganography came into existence which is defined as the "hidden writing" that helps to hide the presence ofdata. By doing so, it became quite difficult for intruders to access the dataas it is very difficult to find the difference between the images [6].
In this fig, we can clearly see that the sender is sending a message which is been embedded by a secret key and a stego-image is formed. This process is known as steganalysis, after this the image is further processed and the receiver will extract the image with use of the key. And so, the message will be successfully sent to the receiver.

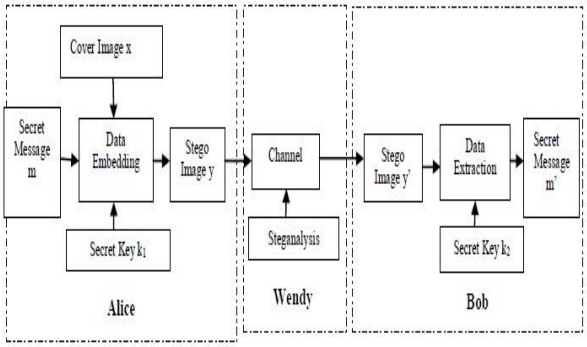

Figure 1.1 The model of steganography and steganalysis[4]

Steganography helps to hide the file in the various form such as image, audio, video, text. And the objective to do this is hiding the existence of data in the cover-image which is unreadable by humans.We have different techniques to implement steganography which will be explained further.
Steganography is utilized in two domains which are spatial domain and frequency domain. In the frequency domain, values of pixelsare changedand then processing is applied whereas in spatial domain, directly processing is done on the pixels.[5]

STEGANOGRAPHY

Steganography comprise of basic three components which are carrier, message and key. The carrier is said to be a picture, MP3 or a TCP/IP packet.[3] And a key is utilized to encode or unscramble a message and the password can be anything, a

pattern or a video. The idea driving steganography is that if a client wants to send a message to collector, the communication between them is constrained by a switch or server. We can watch that sender wishes to send a message to recipient, so to do so it implants it into a spread picture and obtains a stego picture. In a standard definition, this strategy of typifying message isn't known and is kept as a mystery between the two. Be that as it may, it is seen that the algorithm being used isn't a mystery yet the key is mystery between the two, and it is also known as Kerchoff's guideline [8]. It is a technique to secure the touchy information.
Now we have two types of steganography which are explained below.

SPATIALDOMAIN STEGANOGRAPHY

In this kind of steganography, the work is done directly on the pixels. Also, there are many techniques which are provided to us for this purpose. Few of them are explained below-

i. Least significant bit (LSB)
ii. Pixel value differencing (PVD)
iii. Edges based method
iv. Random pixel selection
v. Pixel mapping method
vi. Pixel connectivity method
vii. Pixel intensity or GLV method
viii. Texture based method

i. LSB METHOD: This method was one of the easiest for message hiding. Here the message is hidden in the LSB. By changing the LSB of pixels one can't observe much difference between stego-image and original image.[10]
ii. PVD METHOD: This method was introduced to increase the encapsulating capacity without any artefacts into stego image. In this, the number of encapsulating bits is calculated by deviation of pixel and its neighbour. This method provides us better result compared to other methods. But there is a disadvantage that it can't resist the statistical analysis.[12]
iii. EDGE BASED METHOD: This method conceals hidden data into the pixels that builds up the origin edges of the carrier image. The secret datamay be of any kind and it is usually hidden in the three bitsof the image but only in the one which are identified by this method.
iv. RANDOM PIXEL SELECTION: In this method the datamay be hidden at any place which means that data is hidden in some randompixel. That pixel will beidentified by using Fibonacci algorithm.
v. PIXEL MAPPING METHOD:This method is used forhiding the information of an image. Encapsulated pixels are calculatedby some function which will depend on the pixel intensity value of the main pixel and the neighbourswill be chosenin the clockwise direction. Data embedding can be done by embedding each bits of the secret message in each of the companion pixel. [14]
vi. PIXEL CONNECTIVITY METHOD:In this strategy, the handling will start at the start of the peak in the image and spreads all through the image. Network gives us that what pixels will be joined to different pixels. The blend of pixels that are connected dependent on connectivity type are called object.
vii. PIXEL INTENSITY METHOD: In this method,we useto embed data by changing the grey level of the image pixels. Here we utilize the strategy for odd and even numbers to insert data in the image. In this technique we perform a coordinated mapping between the binary dataand the pixels in an image.From the image we select the pixels with the help ofa mathematical function.
viii. TEXTURE BASED:Ultimately here the mystery and host images are ordered into squares of fixed size and each obstruct stealthily image is taken as a surface pattern for which the most similar square is found among the squares of the host image.

TRANSFORMDOMAINTECHNIQUES

This strategy utilizes space explicit qualities to insert information and to perform to the picture and change it to area like DCT and DWT. Here the information is installed on the changed picture rather than direct picture.The benefit of this technique is that information can be easily encapsulated where it is less exposed to cropping and processing. And here the component of transformed image spread over the whole image so this helps us from any data attack. But it is a quite difficult way of hiding information. Transform domain techniques are classified into:

i. Discrete Cosine Transform
ii. Discrete Fourier Transform
iii. Discrete Wavelet Transform

iv. Integer Wavelet Transform
v. Discrete Curvelet Transform

i.DCT METHOD:It is a technique for digital image handling and signal preparing which has like high weight ratio, small bit bungle rate, extraordinary information integration ability. This technique allows an image to be isolated into different repeat bands which are high, centreand low recurrence bands and makes it easier to pick the band in which the watermark is to be kept.
ii. DFT METHOD: This technique is very comparable to the DCT strategy however it uses the Fourier transform instead of cosine change; this makes it lack resistance to strong geometric turns.Be that as it may, doing this makes it complex which is very hard to deal with. [15]
iii. DWT METHOD: A wavelet can be portrayed as a wave which oscillates and delays in the time domain.This strategy is a relatively ongoing and a productive system. This strategy has a ton of advantages as it can perform local analysis and multi-goals analysis. At the point when we investigate various frequencies and various goals it is known as multi goals examination. [10]
iv. IWT METHOD: This method makes perceptible embedding more effective. In case of IWT, when the input data contains sequence of integers, the result will no longer be of integers. And hence it is not able to allow perfect making of original image.
v. DCVT METHOD: This method is one of themethods of the multiscale geometric transform. It gives us better edge than that of wavelet so it is an effective method to use in case of image steganography.[9]
These are all the transform domain techniques revised one after other. Now let us go to the conclusion after going through them.

COMPARATIVE ANALYSIS

The table is shown below which shows comparison between different technologies and shows which one is best in which of the following field -

Table 1-

Technique	**domain**	**capacity**	**viability**	**detectability**	**robustness**	**complexity**	**comments**
LSB	Spatial	H	L	H	L	L	Independent of imageformatand texture
MSB	Spatial	M	L	M	L	L	Suitable for high contrastimages
PVD	Spatial	L	L	M	L	L	Preferred for images with objects
EBE	Spatial	H	M	L	L	L	Provides better security
RBE	Spatial	M	L	L	M	M	N/A
Connect	Spatial	M	L	L	M	M	Preferred for mosaicimages
PI(GLV)	Spatial	M	L	L	L	L	Robust hiding for noisy images
Texture	Spatial	M	L	M	M	M	Preferred for patterned
DCT	transform	M	L	L	M	M	Simplest in the transformdomain
DFT	transform	M	L	L	M	M	Involves complex calculation
DWT	transform	M	L	L	H	H	Closely matches with human perception

IWT	transform	M	L	L	H	H	Overcomes the rounding off losses
DCVT	transform	M	L	L	H	H	Improves the degradationat edge areas

CONCLUSION

This paper gives us a review of various steganography procedures from basic to ongoing employments. It also shows us the comparison of various methods intotabular structure on the basis of capacity, viability, detectability, vigorand unpredictability. The analysis shows that transform domain are best for attack frameworks with low data capacity and higher multifaceted nature while spatial is best for restricted unpredictability frameworks also gives many choices for methods choice for framework with constrained computational powers.

REFERENCES

[1] Ammad Ul Islam, FaizaKhalid, Mohsin Shah, ZakirKhan, ToqeerMahmood, AdnanKhan, UsmanAli, MuhammadNaeem "An Improved ImageSteganography Technique based on MSB using Bit Differencing", The Sixth international conference on Innovative Computing technology (2016)

[2] IanMcAteer, AhmedIbrahim, Guanglou Zheng, WenchengYangandCraigValli "Integration of Biometrics andSteganography: A Comprehensive Review" (2019)

[3] Ying Zou, Ge Zhang, Leian Liu "Research on imagesteganographyanalysisbased on deep learning" (2019)

[4] Ra'adA. Muhajjar, FarahA. Badr "Secure DataCommunications using Cryptographyand IPv6 Steganography", InternationalJournal of Engineering & Technology, (2019) 163-168

[5] Ning Wu, PoliShang, JinFan, ZhongliangYang, Weibo Ma, Zhenru Liu "Research on Coverless Text SteganographyBased on Single Bit Rules",IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 022077

[6] U. A. Md. EhasnAli, Md. Sohrawordi, Md. Palash Uddin "A Robust and Secured ImageSteganography using LSB andRandom Bit Substitution",AmericanJournal of Engineering Research (AJER) 2019 Volume-8, Issue-2, pp-39-44

[7] RashaThabit "Improved Steganography Techniques for Different Types of Secret Data" (2019)

[8] ManishaVerma, Hardeep Singh Saini "Analysis of Various Techniques for AudioSteganography in Data Security", IJSRNSC Volume-7, Issue-2(2019)

[9] PranayKalamkar, MrunaliGaikwad, Sumit Gore, DhananjaySonule, Prof. VidyaBodhe "A Review on ImplementationVisualCryptographyandSteganography" (2019) IJSRST, Volume 6, Issue 2

[10] AditiSharma, MonikaPoriye, Vinod Kumar "A Secure Steganography Technique Using MSB", InternationalJournal of Emerging Research in Management&Technology 2017, Volume-6, Issue-6

[11] FarshadMiramirkhani, Omer Narmanlioglu "A Mobile Channel Model for VLC andApplication to Adaptive System Design", IEEE communications letters, vol. 21, no. 5, may 2017

[12] AkramAbdelQaderandFadelAlTamimi "A novel imagesteganographyapproach using multi-layersdctfeaturesbased on support vector machineclassifier", The InternationalJournal of Multimedia& Its Applications (IJMA) Vol.9, No.1, February 2017

[13] SoumenduChakraborty&Anand Singh Jalal&CharulBhatnagar "LSB based non blind predictive edge adaptiveimagesteganography", Multimed Tools Appl (2017) 76:7973–7987

[14] ApoorvaShrivastavaand Lokesh Singh "A new hybrid encryption andsteganography technique: a survey", InternationalJournal of Advanced Technology and Engineering Exploration, Vol 3(14) 2016

[15] AnupriyaAryaandSaritaSoni "ALiterature Review on Various Recent Steganography Techniques", InternationalJournal on Future Revolution in Computer Science &Communication Engineering Volume: 4 Issue: 1 (2018)