International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

A Study and Literature Review on Various Image Steganography Techniques

Sonali K. Powar[1], H.T. Dinde[2], Radhika.M. Patil[3]

[1]*Assistant Professor, Modern College Ganeshkhind Pune (M. S.) INDIA*
[2]*I/C Principal Karmaveer Bhaurao Patil College,Urun-Islmapur (M.S.) INDIA*
[3]*Assistant Professor, Vivekanand College, Kolhapur (M.S.), INDIA*

Abstract- *Now a day's internet plays vital role in communication. Security is major issue while transferring data over internet. The steganography used to send secret data securely to another end. This paper includes review of different image steganography techniques. Every steganography technique has it own key features and limitations. Image steganography can hide secret text, image, audio or video inside cover image. This paper includes types of steganography, various steganography techniques like special domain, frequency domain, spread spectrum, masking and filtering and distortion.*

Keywords- Steganography, Data hiding, Spatial domain, Frequency domain, Steganography review.

1. INTRODUCTION

Now a day's internet is used in large amount to communicate with one another. So large number files are transferred on internet for communication purpose. Security is important while transferring data on internet. The cryptography and steganography are used for information security purpose. In cryptography key used to encrypt and decrypt secret message. Sender used key to encrypt secret information and receiver used key to decrypt secret information. The advantage of cryptography is, no one can decrypt message without key. But when secret data is encrypted it converts normal message to meaningless form.

Example: Suppose Secret message is "HELLO" is encrypted using substitutional cryptography like replace H by U, E by R, L by Y and O by B. The resultant encrypted message is "URYYB". This encrypted message is meaningless. So, the disadvantage of cryptography is, looking at encrypted message anyone can say that there must be a secret message hidden inside it. It means the cryptography attracts intruder's attention. This drawback is overcome in steganography. The steganography hides the existence of secret message so that no one can detect its presence [5][7].

Steganography means hidden secret data with in another carrier medium. The carrier medium can be text, image, audio or video. In embedding processes secret data is embedded into carrier medium and in decoding processes secret data is extracted from carrier medium. For more security purpose both techniques i.e. cryptography and steganography are combined together. The secret data is encrypted first and then embedded into carrier medium. At the receiver side data is extracted from carrier medium and then decrypted to get secret data. The steganography algorithm with high capacity and high imperceptibility is a good steganography algorithm.

2. STEGANOGRAPHY

In ancient Greek used wax table to hide message. "The person would scrape wax off a tablet, write secret message on the underlying wood and again cover the tablet with wax to make it appear black or unused" [6]. Another method was massager's head was shaved and secret message was tattooed on his head. After the hair grew back message was send to destination where head was shaved to see secret message. Early in the World War II invisible ink was used to write secret message. Invisible ink was used to write secret message between lines of innocent letter. Secret data was also hidden in document itself. Innocent message was written in document but actually secret data was present in it. By extracting specific position letters data would be retrieved. "During world war II introduced microdots. Microdots where complete document, picture, plans reduced in size to the size in period and attached to the common paper" [8].

In digital steganography data is hidden in carrier medium like text, image, audio or video. Depend upon carrier medium used in steganography algorithm, the steganography is divided into different types as shown in figure 1

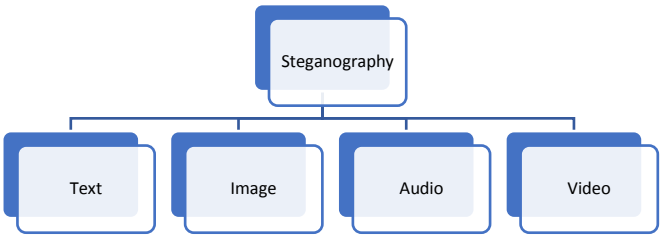

Figure 1: Types of Steganography

2.1 Text Steganography

In Text steganography text file used to hide secret data. In this method secret letter is hide in every n^{th} letter of carrier text file. It is faster as text file requires less amount of memory. It is easier method for secret communication.

2.2 Image Steganography

In this method secret information is hide into image called as cover image. In cover image data is hide using steganography algorithm to get stego image. In this type if large amount of data is embedded into cover image, it will create more distortion in image and it will be susceptible to visual attacks. So, in this type of steganography to obtain good result the algorithm has to balance capacity and amount of distortion.

2.3 Audio Steganography

In this method audio file is used as a carrier medium. This method is more robust it means it is able to resist different attacks. The limitation of this method is less mount of data can be embedded. This method uses WAV, AU, MP3 sound files to hide data. Low bit encoding, Phase encoding and spread spectrum are some audio steganography methods.

2.4 Video Steganography

In video steganography secret data is stored in video file. Video is combination of pictures. DCT frequency transformation is generally used hide secret data in images of video. This type of steganography is more robust. Video steganography uses MPEG, AVI etc. file formats to hide secret data.

3. IMAGE STEGANOGRAPHY TECHNIQUES

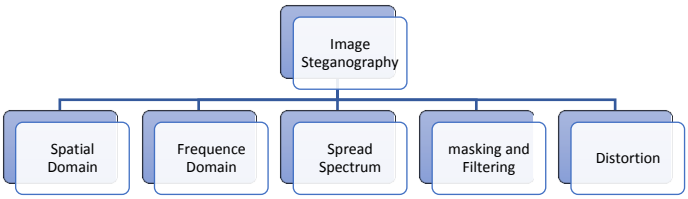

Figure 2: Image Steganography Techniques

The figure 2 shows various image steganography techniques. Most commonly used steganography techniques are special domain and frequency domain.

3.1 Spatial Domain

In Spatial domain approach data is directly hide in pixel value. Most common spatial domain techniques are LSB and PVD. In LSB technique data is hide in least significant bit of cover image pixel. As change in LSB value of pixel does not creates large difference so LSB is used in embedding process. This method provides good capacity but not more robust. In case of PVD technique difference between two consecutive pixels is used to calculate payload value. If difference is more, more bits can be stored. So, using PVD more data is stored in edge region and less data is stored in smooth region.

3.2 Frequency Domain

In frequency domain technique instead of hiding data directly into pixel, first image is transforms into frequency domain and then data is hide in transformation domain coefficient. This technique provides less capacity but it is more robust than spatial domain technique. Most commonly used transformations are DCT, DWT, DFT.

3.3 Spread Spectrum

In this technique secret data is spread over wide frequency bandwidth. This technique provides very good robustness. If signal to noise ratio in every frequency band is small then it is difficult to detect presence of secret data. “Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data” [9].

3.4 Masking and filtering

This technique used to hide data in 24 bit or gray scale image. In this technique data is hide by creating mark in cover image. So, it is similar to watermarking. This

technique used most significant part of image to hide the data so it is more robust against compression.

3.5 Distortion

. "Encoder add sequence of change to cover image. So, information is described as being stored by signal distortion" [10]. The secret data is extracted using difference between cover image and stego image.

4. LITERATURE SURVEY

Chakraborty, Jalal and Bhatnagar in 2013 proposed algorithm which distribute secret data (payload) across different matrices to achieve same visual distortion. Data is embedded in second least significant bit plane using XOR operation. The limitation of this method is maintaining different matrices [11]. Sarreshtedari and Akhaee, 2014 proposed method to enhance visual imperceptibility by reducing distortion in cover image. This method provides 1 bit per pixel embedding capacity with 1/3 pixel modification. This method resists against LSB detection attacks i.e. HCF-COM. The limitation of this method is less embedding capacity [12]. Qazanfari and Safabakhsh, 2014 proposed GLSB++ method. They introduced lock key. Best lock key is calculated according to cover image. Using lock key some cover elements are locked which will not be used to hide the data. In this method some extra bits are embed in cover image to preserve histogram of cover image. This method improves image quality and also provides resistance against histogram and chi-square attack [13]. Yuan, 2014 uses multiple covers to embed data. In this method "secrete bits shares among edges, texture regions of cover according to gradient based embedding distortion measure, also this method used to hide location sensitive secrete (e.g. meaningful secrete image)" [14].

Uma Maheswari and Jude Hemanth poprosed method in 2015 in which they use Fresnelet transform (FT). LSB of High frequency sub-bands are used to embed data. OR code is used to enhance the security of secrete message. "The average PNSR of this method is 45.40 Db and embedding capacity is 352,332 bits" [1]. Raja, Chowdary, Venugopal and Patnaik enhanced security using LSB, Discrete Cosine Transformation (DCT) and compression technique. In this method first data is embed into cover image using simple LSB method to get stego image. DCT is applied on stego image and then using quantization and run length coding algorithm stego image is compressed to increase security. Using this method secure images with low MSE and BER are transferred without using any password, in comparison with earlier works." [2]. "Genetic Algorithm and Optimal Pixel Adjustment Process used to obtain an optimal mapping function which helps to reduce the difference error between the cover and the stego-image" [3]. So, using optimal mapping function, more data can be embedded with low distortion. DWT frequency transformation is used to increase robustness of method. This method achieved 39.94 dB PNSR value at 50% of embedding capacity.

A, S and P.P, 2010 The M x N gray scale image is divided into nonoverlapping 8 x 8 blocks and 2D DCT is applied on each block. LSB of DCT coefficients are used in embedding process. Huffman encoding is applied on secret message before embedding into DCT coefficients. At receiver side Huffman table is require to extract secret data so this method provides satisfactory security. Use of frequency domain and Huffman encoding provides robustness. This method achieved the PSNR near about 50 Db [4].

Po-Yueh Chen and Hung-Ju Lin proposed method in which low frequency sub band LL of DWT transformation is remain untouched to maintain image quality. Data is embedded in two modes fixed (fixed bits per pixel) or variable. While embedding key matrix is generated which is also embed in image. Data cannot be extracted without key matrix. This method gives satisfactory PSNR values for higher capacity [15]. Amitava Nag, et al. uses Huffman encoding to encode secrete message. DWT frequency transformation is applied on cover image. Data is embedded in high frequency region of image [16]. Atawneh et al., 2016 proposed method in which secrete image is converted into base 5 and the using DE scheme it is embedded into cover. This method is more robust but provides less embedding capacity [17]. The algorithm invented by Baby et al., 2015 can store 3 secrete images into colored cover image. DWT is applied on cover image and secrete images up to N level. Only LL bands of secrete images are stored in cover image. So, method provides more embedding capacity but takes more execution time [18].

Satish et al., proposed method in 2004 which uses chaotic encryption and chaotic modulation in spread spectrum image steganography. This method is less expensive. It can be used in privacy and security of commercial consumer electronic products. Interleaving the message using a chaotic sequence increases robustness of method [19]. Yadav and Dutta, 2017 proposed method which provides 3 level security. In first level RSA Encryption with Diffie-Hellman Key exchange is used to encrypt secret message. In second level data is compressed using Run-length encoding. In third level pseudo generator is used to spread over cover media. This method results 71.347 dB, 0.0048 MSE at 0.5 compression ratio and BER of 0.0171 [20].

5. CONCLUSION

This paper contains literature review of different steganography techniques used to transmit secret information securely through internet. Every technique has

its own advantage and disadvantage. The Spatial domain technique provides good capacity but not robust against different attacks. The frequency domain technique provides good robustness but less embedding capacity. Making technique are robust against compression.

REFERENCES

[1] Uma Maheswari, S. and Jude Hemanth, D., 2015. Frequency domain QR code-based image steganography using Fresnelet transform. AEU - International Journal of Electronics and Communications, 69(2), pp.539-544.
[2] Raja, K., Chowdary, C., Venugopal, K. and Patnaik, L., 2005. A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. 2005 3rd International Conference on Intelligent Sensing and Information Processing.
[3] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi. High Capacity Image Steganography using wavelet transformation and Genetic Algorithm. Proceeding of the International MutliConference of Engineering and Computer Scientists 2011 Vol I, IMECS 2011, March 16-18,2011, Hong Kong.
[4] A, N., S, B. and P.P, S., 2010. A novel technique for image steganography based on Block-DCT and Huffman Encoding. International Journal of Computer Science and Information Technology, 2(3), pp.103-112.
[5] Provos N. and Honeyman P, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.
[6] Johnson, N. and Jajodia, S., 1998. Exploring steganography: Seeing the unseen. Computer, 31(2), pp.26-34.
[7] F. Piper, "Basic Principles of Cryptography", IEEE Colloquium on Public uses of Cryptography, pp. 2/1-2/3, April 1996.
[8] Alan Siper, Roger Farley and Craig Lombardo. The rise of steganography. Proceeding of Student/Faculty research day, CSIS, Pace University, May 6th 2005.
[9] Anupriya Arya, Sarita Soni. A Literature Review on Various Recent Steganography Techniques. International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 4 Issue: 1
[10] H.S. Majunatha Reddy and K.B. Raja. (2009)."High capacity and security steganography using discrete wavelet transform. " International Journal of Computer Science and Security. pp. 462-472.
[11] Chakraborty, S., Jalal, A. and Bhatnagar, C., 2013. Secret image sharing using grayscale payload decomposition and irreversible image steganography. Journal of Information Security and Applications, 18(4), pp.180-192.
[12] Sarreshtedari, S. and Akhaee, M., 2014. One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme. IET Image Processing, 8(2), pp.78-89.
[13] Qazanfari, K. and Safabakhsh, R., 2014. A new steganography method which preserves histogram: Generalization of LSB++. Information Sciences, 277, pp.90-101.
[14] Yuan, H., 2014. Secret sharing with multi-cover adaptive steganography. Information Sciences, 254, pp.197-212.
[15] Po-Yueh Chen and Hung-Ju Lin. A DWT Based Approach for Image Steganography. International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.
[16] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar. A Novel Technique for Image Steganography Based on DWT and Huffman Encoding. International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6)
[17] Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P. and Gupta, B., 2016. Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimedia Tools and Applications, 76(18),
[18] Baby, D., Thomas, J., Augustine, G., George, E. and Michael, N., 2015. A Novel DWT Based Image Securing Method Using Steganography. Procedia Computer Science, 46, pp.612-618.
[19] Satish, K., Jayakar, T., Tobin, C., Madhavi, K. and Murali, K., 2004. Chaos based spread spectrum image steganography. IEEE Transactions on Consumer Electronics, 50(2), pp.587-590.
[20] Yadav, P. and Dutta, M., 2017. 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio. 2017 Fourth International Conference on Image Information Processing (ICIIP).