International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 5 (2014), pp. 485-490

http://www. irphouse.com /ijict.htm

Review On Secrete Sharing Scheme for Color Image Steganography

Tanuja Mahajan[1], Bhakti kurhade[2] and A. Mahajan[3]

[1, 2, 3] Department Of Computer Science and Engineering,
[1]Student, G. H. Raisoni Academy of Engineering and Technology, Nagpur, India.
[2] G. H. Raisoni Academy of Engineering and Technology, Nagpur.
[3]Priyadarshini College of Engineering, Nagpur, India.

Abstract

When we send data through internet it is necessary to protect this information while communication. For security purpose concept of cryptography and steganography is being used. Secrete writing is known as cryptography. Steganography is the method in which existence of the message can be kept secret. In this paper, we clarify on what steganography is its importance as well as review on the different techniques used in implementing steganography. This Review helps us to proceed in the right direction of research in color image steganography.

Keywords: Cryptography, steganography, LSB, Hash-LSB, cover image, stegano image.

1. Introduction

In today's world communication is very important factor. We do communication through different medium such as languages, telephone, internet etc. but it is not fully secure. For security purpose concept of cryptography and steganography is being used. Cryptography is a technique which convert message in unreadable form during communication.

The word steganography derived from the Greek word *Steganos*, which mean covered or secret and *graphy* mean writing or drawing. Therefore, steganography means covered writing. Steganography is the art and science of hiding information such way that its presence cannot be detected and a communication is happen. Cryptography hides the contents of a secret message from hackers, whereas

steganography even hide the existence of the message. Steganography does not alter the structure of the secret message, but hides the message inside a *cover-image* so it cannot be seen with necked eyes. In steganography we use cover image, stegano image.

Cover image- image in which another image is hidden.

Secrete image- image which is hidden in cover image.

1.1 Basic Model of Steganography

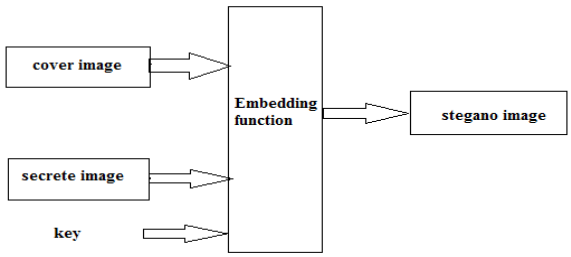

Fig. 1: Basic model of steganography.

In fig 1 we take cover image then take secrete image & key and embedding these two images then we get stegano image which is similar to our cover image.

1.2 Kinds of Steganography-

There are four kinds of steganography they are as follows

1.2.1 Text

1.2.2 Image

1.2.3 Audio /Video

1.2.4 Protocol

1.2.1 Text Steganography-

It uses the text media to hide the data.

1.2.2 Image Steganography-

In this images are used as cover object i.e. to hide data.

1.2.3 Audio steganography-

When secret data is embedded into digital sound, the technique is known as audio steganography. Secret message is embed in WAV, MP3 sound files.

1.2.4 Protocol steganography-

In this method we use protocol to transfer data and for hiding.

2. Current Approaches

Existing Cryptography Algorithm-

There are so many algorithm exist for encryption and decryption they are as follow

1) Symmetric Algorithm or Private Key- Uses a single key for both encryption and decryption.

2) Asymmetric or public key Algorithm- Uses one key for encryption and another for Decryption.
3) Hybrid Cryptography-Combination of symmetric and asymmetric algorithm.

2.1 Different Steganographic Technique-

2.1.1) spatial domain Technique
2.1.2) Transform domain techniques
2.1. 3) Spread spectrum techniques
2.1.4) Statistical method
2.1.5) Distortion techniques

There are so many steganographic techniques but we generally use first two techniques.

2.1.1 Spatial Domain Technique –

In Spatial domain, first decomposed cover-image into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. It generally uses LSB algorithm or BPCS algorithm Advantages are high embedding capacity, easy to implement.

2.1.2 Transform domain technique-

In Transform domain, we embed information in frequency domain of the transformed image. Advantage of this domain is to hide the image in the area that is less exposed to the compression and image processing. This technique runs on both lossy and lossless image. It generally uses DCT, DFT, and Wavelet Transformation.

3. Related Work

There are so many steganographic techniques which are used for hiding data within image. In paper [1] optimized strategy is discussed that uses genetic algorithms to find the best mapping function between cover image and secret data. If iterations are big then this approach cannot be completed in polynomial time. In paper [2] comparison of high capacity filter with low capacity filter is discussed that produces steganography technique to embed the data. Paper [3] presented research work on data hiding in images by hybrid LSB substitution technique. It is the method of Optimal LSB substitution with OPAP.

Paper [5] presented pixel-value differencing image steganography method to increase the capacity of the hidden secret information and to provide a stego-image. This method uses the largest difference value between the other three pixels close to the target pixel. Paper [8] propose (N, 1) Secret Sharing Approach Based on Steganography with Gray Digital Images method which contain an embedding and an extraction algorithm. This proposed scheme basically uses an Exclusive-OR (XOR) operation and a binary-to-gray code conversion.

In paper [9] least significant bit (LSB) insertion technique is discuss. It is simple approach to embedding information in a cover image. In this method we embed 8th bits of data at (LSB) of each pixel in the cover image in order of 3,3,2 respectively. The altered image is called stego-image. Paper [11] “On the Limits of Steganography”,

presented number of attacks on information hiding scheme and suggested improved embedding efficiency and public key steganography.

Paper [12] proposes novel approach to develop a Secure Image based Steganographic Model using Integer Wavelet Transform. In paper [14] designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used.

In Paper [16] we discuss image steganography technique based on Integer Wavelet Transform (IWT) .IWT converts spatial domain information to the frequency domain information. We use assignment algorithm for embedding secret data and for best matching between blocks.

4. Evaluation and Discussion

Analysis drawn from comparative study of each of the algorithm is shown in following table.

Table 1: Comparative study

No	Technique	Advantages	Disadvantages
1	LSB	1 Simple to implement 2 undetectable by the average human if done	1. Less secure.
2	Jsteg	1.Better stegno size 2. Quality of stegno image is best.	1. stego-size result is poor.
3	JMQT	1.Better Capacity 2. More data embedding.	1. Large stegno size.
4	HSLB	1. Provide more security. 2. Embedding capacity of the technique is more. 3. Improve performance.	1. Compressed file must be decompressed first.

In above table we compare different steganographic algorithm. Proposed Hash LSB gives better embedding capacity with preserving quality of the image.

5. Applications

- Mobile Banking
- Military
- Intelligence agencies
- smart identity cards
- Medical Imaging
- Online voting
- Enable secrete communication

6. Conclusion

Analysis has been conducted by using number of different steganographic algorithm such as transform domain and spatial do-main etc. Spatial domain techniques are easy to implement and have high payload as compare to transform domain technique. So we conclude that there are large number techniques for implementing image steganography but when we combine spatial domain technique with hash function and cryptography together then it provides two levels of security and better quality image. It is quite impossible for hackers to steal the data.

7. Acknowledgments

It is our privilege to acknowledge with deep sense of gratitude towards our seminar guide Dr. A. Mahajan and our seminar co-guide Prof. Bhakti kurhade for their valuable suggestions and guidance throughout course of study and timely help given for doing this literature review.

References

[1] A.M. Fard, M. Akbarzadeh-R., and F. Varasteh-A. (2009), "A new genetic algorithm approach for secure JPEG steganography", in Proc. of *IEEE International Conference on Engineering of Intelligent Systems ICEIS*, **vol 60**, *No 1*, pp. 216-219.

[2] Babita Ahuja and Manpreet Kaur(2009), "High Capacity Filter Based Steganography", *International Journal of Recent Trends in Engineering*, **Vol. 1,** *No. 1*,pp510-514.

[3] Chin-Chen Chang, Hsien-Wen Tseng (2009), "Data Hiding in Images by Hybrid LSB Substitution", *Third International Conference on Multimedia and Ubiquitous Engineering*, **vol 3**,*No 2* pp- 360 - 363

[4] Gandharba Swain, Saroj Kumar Lenka (2010), "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels", Proceedings of the *International Conference on Communication and Computational Intelligence*, Kongu Engineering College, Perundurai, Erode, pp.529-534.

[5] Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xiong (2009), "Image Steganography using Pixel-Value Differencing", *Second International Symposium on Electronic Commerce and Security*, pp- 109 - 112.

[6] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir (2008), "A New Image Steganography Technique", *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp-1-4

[7] J.G.Yu1, E.J.Yoon2, S.H. Shin1 and K.Y. Yoo (2008), "A New Image Steganography Based on 2k Correction and Edge-Detection", *Fifth International Conference on Information Technology*, pp. 315-319

[8] Jinsuk Baekl, Cheonshik Kim, Paul S. Fisherl, and Hongyang Cha (2010), "(N, 1) Secret Sharing Approach Based on Steganography with Gray Digital Images", *IEEE International Conference, Wireless Communications, Networking and Information Security (WCNIS)*, pp-325 – 329

[9] M. S. Sutaone, M.V. Khandare (2008), "Image Based Steganography Using LSB Insertion Technique", *IET International Conference on Wireless, Mobile and Multimedia Networks*, pp-146 – 151

[10] R. Ji, H. Yao, S. Liu and L. Wang (2011), "Genetic Algorithm Based Optimal Block Mapping Method for LSB Substitution", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 215-218

[11] Ross J. Anderson and Fabien A. P. Petitcolas (1998), "On the Limits of Steganography", *IEEE JOURNAL on selected areas in Communications*, **VOL. 16,** *NO. 4***,** pp- 474 - 481.

[12] Souvik Bhattacharyya, Avinash Prasad Kshitij, Gautom Sanyal (2010), "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform", *International Conference on Recent Trends in Information, Telecommunication and Computing* ,pp- 173-178.

[13] Sunny suchdeva and Amit Kumar (2012), "Color Image Steganography Based on Modified Quantization Table", *in 2nd international conference on advance computing and communication tech*, **vol 51**, pp. 534-538

[14] Wuling Ren, Zhiqian Miao (2010), "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", *IEEE Second International Conference on Modeling, Simulation and Visualization Methods*, pp-221-225.

[15] Yi Luo, Xiaolong Li, and Bin Yang (2011), "Locating steganographic payload for LSB Matching embedding ", *IEEE transaction on computers*, **vol 2, no 1,**pp.214-218

[16] N.Raftari (2012), "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", *Sixth Asia Modeling Symposium.*, pp.523-527