A Review: On Various Image Steganography Approaches In Data Security And Transmission

Harpreet Kaur
M.Tech. Student
CSE Dept.
Ramgarhia Institute of Engineering and Technology
Punjab, India.
1182bains@gmail.com

Varinderjit Kaur
M.Tech. HoD
CSE Dept.
Ramgarhia Institute of Engineering and Technology
Punjab, India.
Vari006rupi@gmail.com

Dr. Naveen Dhillon
Principal
Ramgarhia Institute of Engineering and Technology
Punjab, India.
principal@riet.ac.in

Abstract— **Steganography has become a popular trend among all of the fields where the security of the data is the major concern. In steganography, the cover file is used to hide the sensitive information. In this case, the cover image can be of text, image, audio or video in nature. In this work, the author has defined the basics terms related to the steganography such as applications of steganography, techniques used for steganography. The work that has been done in past for increasing the efficiency of the final stego image is also defined in this. For this purpose, various steganographic mechanisms are used and LSB, encryption, cryptography etc are the major ones.**

Keywords*— *image security, image steganography, Least significant bit

I. INTRODUCTION

The word “steganography” is derived from Greek words i.e. “stegano” stands for cover and “graph” stands for writing. Thus, the word steganography defines the whole process of hiding the data behind a cover file whether it is audio, video, text or image [1]. Steganography can also be defined as an art or science for securing the confidential information from third party or malicious users who are not authorized to have an access to the information. In steganography the data is hidden behind a cover file and the process of data hiding can be done by using various techniques such as encryption keys, cryptography and others like Least Significant Bit (LSB), wavelet domains etc [2].

Steganography is applicable in wide range of fields. Following are some of the applications of steganography:

a) Secret communication [3]: steganography is used for establishing the secret communication where the sender and receiver of the message do not want to disclose the information attached in message. In this, secret messages, blueprints or other sensitive information can be transmitted without notifying the attackers or intermediates.
b) Copyright Protection is another domain where the steganography is highly preferred. Steganography is applied on digital form of copyrights generally to prevent it from any digital theft, attack or from being copied [4].

II. STEGANOGRAPHY TECHNIQUES

Steganography uses various techniques and methods for hiding the data behind a cover image. Following is the classification of image steganography methods:

1. Spatial Domain based image steganography
2. Frequency Domain based image steganography
3. Masking and Filtering

The methods such as LSB falls under the category of spatial domain and the mechanisms such as Discrete Cosine Transform, Discreet Wavelet Transform, and Discrete Fourier Transform are kind of frequency domain based steganography techniques. Following table represents the traditional work with respect to the techniques used for steganography by the authors.

Table 1 Review to the techniques used for Steganography

Techniques	Author	Name	Description
LSB	G. Prashanti et al. [11] 2015	A new Approach for Data hiding with LSB Steganography	This study provides a survey on various achievements on LSB based image steganography. Along with this, the author had also discussed the advancements that has been done to increase the performance of the traditional LSB method. A novel approach for image steganography is also developed by

			the author.
LSB	Savita Goel et al. [12] 2015	Image steganography-Least Significant Bit with Multiple Progression	A novel data embedding technique has been proposed in this study by using the LSB scheme with various progressions. On the basis of the experimental results, it is concluded that the proposed work is more efficient, fast and reliable in comparison to the traditional mechanism.
DWT	Della Baby et al. [13] 2015	A Novel DWT based Image Securing method using Steganography”	The study proposed a mechanism for image steganography by using more than one RGB images to single RGB image. The DWT mechanism is applied for the purpose. The results conclude that the proposed work is little perfect than the traditional work with high data embedding capacity as it leads to the variations in stego image.
Masking and Distortion	Bingwen Feng et al. [14] 2015	“Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”	The author developed a mechanism for binary image steganography. The objective of this technique is to decrease the effects of distortion on pattern of the image. Along with this, a measurement scheme is also proposed by the author. After experiments, the proposed work is found to be highly secure, statistical efficient and has the high data hiding capacity.
Heuristic Genetic Approach	M. Nusrati et al. [15] 2015	“Steganography in image Segments using Genetic Algorithm”	The author have defined a new method for image steganography by using the advanced heuristic genetic algorithm in order to optimally locate the appropriate in cover image for hiding the data.
LSB	K. Qazanfari and R. Safabakhsh et al. [18] 2014	A new steganography method which preserves histogram: Generalization of LSB++”	A new version i.e. LSB++ has been proposed in this work. The objective of using LSB++ is to retain the histogram so that the histogram based attacks can be found. The invention of this technique

			eliminates the embedding of extra bits as done in traditional LSB mechanism.
Huffman Encoding+ LSB	Amitava Nag et al.[19]	“A Huffman Code Based Image Steganography Technique”	The steganography method proposed in this work is based on Huffman encoding mechanism and LSB. The Huffman encoding is applied for encryption purpose and LSB is applied for hiding the data behind the cover image.
LSB+Bit inversion	N. Akhtar et al. [20] 2014	An Improved Inverted LSB Image Stegano-graphy”	The developed mechanism is based on bit inversion and LSB technique.

III. RELATED WORK

Sahar A. El_Rahman, [5] steganography is an art of obscuring the communication by hiding the transmitted message in a cover file such as video, audio, text, image etc. In this work, the DCT is used for steganography process by using the LSB for hiding the sequential bits. The performance of the proposed work was measured and analyzed in the terms of PSNR and MSE on both low and middle frequency. On the basis of the observed results, it was concluded that the middle frequency has the highest data hiding capacity with higher PSNR and MSE in comparison to the low frequency. The proposed work is implemented for hiding the data regarding nuclear reactors. The findings of the study depicts that the proposed work has high data embedding capacity without any distortion to the final image.

K. Thangadurai [6], represents an overview to the to the LSB mechanism for data hiding behind image file. Along with this, the study also analyzes the research work on data steganography by using cryptography. The author depicts that the steganography is a done to enhance the security of the data by hiding it behind a cover file. In steganography, the hidden data is not visible to the human until and unless he is not familiar with the steganographic mechanism used for embedding the data. Thus, the person with the encryption key can decrypt the encrypted message. The author had also stated that the LSB is the quite efficient mechanism for hiding the data.

Sahib Khan [7], (2015), introduced the edge based data hiding technique. The development was done to take benefit of less sensitivity of human visual corresponding to the complex region of image. The proposal was done by utilizing the edge detection and steganography techniques. The author implements the canny edge detection mechanism in order to find out the true edges in the image. Along with this, the 4LSB data embedding technique is used to hide the data in 4 least significant bits of the detected edges in the images. The reason behind embedding the data behind the edges is to enhance the quality of the final stego image. On the basis of the experimental results, it was concluded that the proposed work has 4% more data hiding capacity in comparison to the traditional data hiding technique.

Bassam Jamil Mohd[8], (2012), introduced a hardware model by using LSB mechanism in a cyclone II FPGA of Altera sequence. The model had been developed by implementing the Nios embedded processor. The designed model balances the tradeoff between imperceptibility, quality and capacity of the produced output. The proposed work comprised of high computations thus, it leads to the high accuracy with speed up process of steganography.

Gotfried C. Prasetyadi [9], (2017), developed steganography mechanisms to hide a computer file behind a cover file that is also a type of computer file. The append insertion mechanism was used for generating the stego image. The append insertion was utilized to overcome the issue of message format of various prominent steganography techniques. The AES-256 is applied for encrypting the secret message. In this, a specific block of bytes was used for identifying and verifying the original information so that the recovery of the message can be done while preserving the integrity. The implementation of the proposed work was done by using C# and .NET programming framework. In this whole process, single cover file comprises of exactly one message. While testing of the proposed work, the 5 files were selected randomly as a secret message. Then the SHA-256 was implemented for evaluating the integrity in both cases i.e. before hiding the data and after recovering the data from stego file. The results concluded that the proposed work retains the integrity of the confidential messages by exact has value.

Fatema Akhter [10], (2016), the author represents the mechanism for graph steganography (Graphstega). In this form, the message is converted to the plotted data in graphs. The graphs are daily used in every domain for the purpose of analyzing and evaluations. Graph stega embeds the secret messages without arising any kind of suspicion. The author introduced a graphstega approach to develop a secure method for hiding the message in an unnoticeable manner so that the data could be secured from malicious attacks. The proposed work is efficient than traditional graphstega approaches as it performs the word by word conversion instead of letter by letter conversions by using Huffman encoding.

IV. CONCLUSION

Now a day, the data transmission takes place in electric format by using the facilities provided by the internet or networking. Therefore, there are high possibilities that the confidential information could be hacked or attacked by the malicious users. Hence to securing the sensitivity data becomes priority now days. For this purpose, this work is organized to represents a brief overview to the steganography and its various methods. This study also covers the traditional work that has been developed for enhancing the productivity and quality of steganographic techniques. On the basis of the li8terature work, it is concluded that the LSB is the prominent method used for steganography. Thus, in future, more amendments could be done in LSB mechanism.

REFERENCES

[1] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 2013.

[2] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 2013.

[3] Lin Zhang, Jianhua Wu, Nanrun Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.

[4] Parmar Ajit Kumar Maganbhai1, Prof. Krishna Chouhan2, "A Study and literature Review on Image Steganography", IJCSIT, 2015.

[5] Sahar A. El Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", Elsevier, 2016.

[6] K. Thangadurai ; G. Sudha Devi, "An analysis of LSB based image steganography techniques", IEEE, 2014.

[7] Sahib Khan ; Nasir Ahmad ; Muhmmad Ismail ; Nasru Minallah ; Tawab Khan, "A secure true edge based 4 least significant bits steganography", IEEE, 2015.

[8] Bassam Jamil Mohd ; Saed Abed ; Thaier Al-Hayajneh ; Sahel Alouneh, "FPGA hardware of the LSB steganography method", IEEE, 2012.

[9] Gotfried C. Prasetyadi ; Achmad Benny Mutiara ; Rina Refianti, "File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method", IEEE, 2017.

[10] Fatema Akhter, "A secured word by word Graph Steganography using Huffman encoding", IEEE, 2016.

[11] G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer, pp. 423-430, 2015.

[12] S. Goel, S. Gupta, N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions", Springer, pp. 105-112, 2014.

[13] D. Baby, J. Thomas, G. Augustine, E. George, N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), pp. 612-618, 2015.

[14] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, Feb. 2015.

[15] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm",IEEE, pp. 102-107, 2015.

[16] N. A. Al-Otaibi, and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, June 2014, pp. 151-157.

[17] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE, pp. 1-6, 2014.

[18] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier, pp. 90-101, 2014.

[19] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar, "A Huffman Code Based Image Steganography Technique", 1st International Conference on Applied Algorithm (ICAA) , pp. 257-265, 2014.

[20] N. Akhtar, S. Khan and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE, pp. 749-755, 2014.