Research and Development in Image Steganography: A Review

Mayank Kulshrestha
Dept. of CSE
Madhav Institute of Science and Technology,
Gwalior, mayankkulshrestha90@gmail.com

Manish Dixit
Dept. of CSE
Madhav Institute of Science and Technology, Gwalior,
manishdixit@ieee.org

***Abstract* --** Hiding information can be accomplished using different techniques. This paper is a review of various images based hiding of secret data which can be a text or another image. The common framework is not tamper proof. Undoubtedly, the most trustworthy techniques is block-based, edge adaptive and uses a least significant bit approach. This falls in the spatial domain. Cryptography is storing and transmitting the information in such a way that it can only be obtained by authorized receiver.

***Keyword* –** Secret, Edge adaptive, LSB, Spatial domain, Crptography.

I. Introduction

The Steganography is the need of the modern era. The voluminous data are required to be sent to the target recipient over the vulnerable channels like internet. The age old method has been improvised by modern data hiding techniques. The data security is achieved by using Cryptography and Steganography. The word „Steganos" means hidden and „Graphy" means writing or drawing. It means veiled writing. This method has reference in the history. In the modern era it has much more importance. The new application is encapsualating the message under a very simple cover and then sent to the target recipient.

In Fig. 1, the image Steganography uses an image to hide the secret data. Embedding process creates the void for the message in the Cover Image and resultant stego-image is transmitted over the channel.

The sender and receiver have understood there is a secret message of involved key

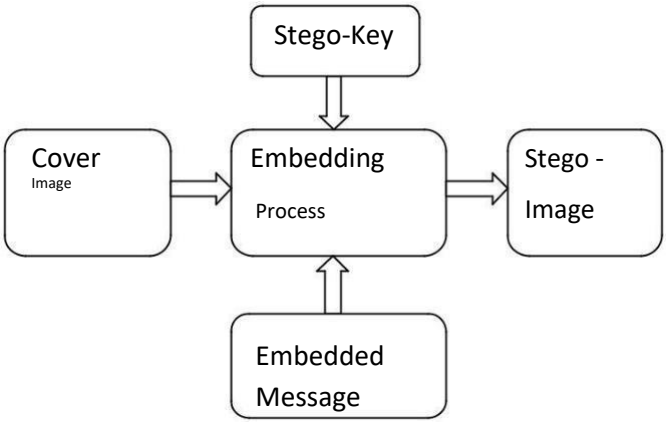

Fig. 1 Embedding Procedure

words through some other reliable channel. The recipient is also informed about hiding and decoding procedure, it is not easy for any intruder to decode the message.

DOI- 10.18486/ijcsnt.2018.7.2.01
ISSN: 2053-6283

II. Related Work

This paper is a review of the research work done in the field of image steganography in the recent past.

Janki Jasani and Sarita Visavalia [1] have propoJed a novel methodology which uses the gray image to hide the secret message. The Haar Wavelet coefficient properties are used to hide message. The arithmetic coding is used to reduce the size of the secret message. The metrics like Peak Signal Noise Ratio (PSNR) and Structural Similarity (SSIM) are used to estimate the quality performance. The author have used the unique alogorithm to enhance the embedding capacity. The performance of the alogorithm can be judged by proper selection of the cover image. The encryption prior to embedding can further improve the security level.

Panda and S.S. et.al [2] have proposed an approach based on alteration of the nieighbouring pixels of the cover image to apatial image. The embedded area looks unchanged and thus security is maintained.

Lindawati et.al [3] have proposed a digital form based Steganography. The method is making the modification in LeastSignificant Bit(LSB). The Steganography is used in encoding and decoding. The Java and Eclipse are used for coding and it can run on Android smartphone.

B.Karthikeyan et.al [4] have proposed a unique method which uses the classical algorithm with Least Significant bit (LSB). Encoding technique to cover the message. This Further makes decoding more difficult for the attackers. DES algorithm applied to encrypt the simple text called as Cryptography. The recipient is supplied the secret decrypting key.

Qi Li et.al [5] have described the content-adaptive image Steganography. It is based on the image textures.A new game theory model has been applied on secondary embedding. The Nash equilibrium is achieved by the use of game theory.The choices are described on the basis occurrence matrix and dot divergence. The pixels are based exclusively on the co-occurrence matrix.

Narvendra panwar et.al [6] have proposed a QR code based cryptographic technique which can applied to secure the information. The authors have embedded encrypted secret messages in the form of QR code with image encoder. This makes the decoding further difficult for the attackers by using Cryptography.

Bajwa, I.S. et.al [7] have described for color image steganography. The hashing approach has been used for data hiding. Here secured images can be transmitted at higher speed using gray scale. This method can support different formats like GIF,BMP,JPEG etc.

Yasmina et.al [8] have proposed the method which can be used for private and public transmission. The Huffman coding is used to hide the secret data and then covering it with some image. The hough transform is applied by detecting the straight line pixels.

Runtong Zhang et.al [9] have described a method based on the planned point tree and information drawn in algorithm. This has been applied in the field of medicine. The patient data is protected by securing the access.

D. Bouslimi et.al [10] have proposed a latest technique of steganography of encipher images for the reason of verifying the consistency of an picture into both encipher and spatial domains. This Techniques added the Quantization Index Modulation (QIM) and Paillier Cryptosystem.

Khodaei, M et.al [11] have proposed a data hiding method by making the use of pixel value differencing and LSB substitution.

The Image is split into two blocks of two successive pixels. The difference of two pixels is calculated, and on the basis of number of embedding bits capacity is estimated into the LSB of two pixels.

Weiming Zhang et.al [12] planned a paper of encipher images. It is essential to secure the confidentiality of messages and manage the message at a similar moment. It is used in reversible steganography in encipher picture. It is used in reversible picture transformation because the new structure for reversible steganography based on reversible picture transformation. The content of the original picture to the content of other picture with equal size is called reversible picture transformation.

Aura Conci et.al [13] have used an AES algorithm to improve the hidden technique to a higher level of security. Path relinking is also used within the AES. This combined strategy yields better result as compared with LSB. This method creates a larger space for data hiding.

Sriram, S et.al [14] have developed a unique method to transmit important data without disclosing it via a private/public channel. The python image library and open CV framework are used for this purpose.

Khan Farhan Rafat et.al [15] have tried to make a secret image difficult to decipher and it depends upon the human visual system. There is an inverse relationship between the data hiding and degree of robustness.

Tomas Denemark et.al [16] have adopted additing side data of the senders end. The

DOI- 10.18486/ijcsnt.2018.7.2.01
ISSN: 2053-6283

precover of high quality id most commonly used. In this work multiple images are used of the same scene in case where cover image is inaccessible to the sender. The tripod based camera image and image obtained from the hand-held camera are used together to improve the robustness of the security. This is supported by Monte Carlo simulation.

Weixuan Tang et.al [17] describes the method which can be applied on gray and color images without any difficulty. The paper describes CMD-C framework (clustering modification directions for color components). The technique is based on continuous change in color components for the same pixel position. The image is fragmented into sub images and then the secret message is sparingly embedded into the image. This strategy shows the improveness over the conventional methods.

Ne matollah Zarmehi et.al [18] work describes the steganalytic framework for digital video. The cover frames are estimated and then compared against the received video frame, based on this residual matrix is calculated bad. The video is scanned by support vector machine and this checks the video for hidden images and in case of the doubt the embedding process is repeated.

Jiang Yu et.al [19] works is based on the COR (contrast of residuals) steganalysis. The fluctuation function is used to find the complex blocks. The residuals have contrast is represented as an angle.

Table I Summarizes The Comparison Between The Related Work For Image Steganograph

S. No.	Author name	Techniques used	Advantages	Disadvantages
1.	Qi Li et.al [5]	Game theoretic model for content adaptive image steganography.	Correct the judgement error.	Limited to grayscale images.
2.	B.Karthikeyan et.al [4]	LSB encoding using the DES algorithm.	Improved security by using cryptography and image stegano.	Distorted target image.
3.	Lindawati et.al [3]	Encryption using LSB techniques and secret key.	Double security using secret key and encryption.	Slow implementation.
4.	Narendra panwar et.al [6]	QR code based on cryptographic techniques using the DES algorithm.	High data representation capacity.	Distortion in the contents.
5.	Yasmina M.A. Abdalnour et.al [8]	LSB, Huffman coding.Use of steganography and cryptography.	Better stego image quality, high PSNR value.	Slow and difficult to find the appropriate cover image.
6.	Runtong zhang et.al [9]	Knowledge-constrained role based access control (KC-RBAC) techniques.	Precise access control.	Lack of flexibility.
7.	D.Bouslimi et.al [10]	Combination of quantization index modulation & the paillier cryptosystem.	Very low image distortion, high capacity to support watermarking.	Vulnerable to attacks, lossy image compression.
8.	Weiming Zhang et.al [12]	Reversible data hiding in encrypted images based on reversible image transformation.	Good image quality & large embedding capacity.	Loss of the image quality.
9.	Khan Farhan rafat et.al [15]	LSB technique, fusion of cover and information.	Secure and aptness of colored image.	Lack of benchmarking for suitable cover image.
10.	Tomas Denemark et.al [16]	Precover jointly quantized and embedded with the secret key.	Low embedding Cost	Poor quality.

DOI- 10.18486/ijcsnt.2018.7.2.01
ISSN: 2053-6283

III. Conclusion and Future Work

Future research is expected to explore horizons beyond the scope of this paper. It is hoped that the limitations of this work would be considered as the beginning for the research in the future. The effectiveness and efficiency of the proposed system can be improved and enhanced in the way of capacity, Security and robustness. Strict algorithm can be performed either privately, or in a public way of embedding the secret message and made them secure and robust, by using the quantization-based hiding for instance. It is difficult to obtain a steganography that satisfies both criteria of high security and high robustness; therefore to find a new mechanism to satisfy our needs is worth to be investigated. To enhance the security and robustness for steganography, the proposed scheme can be employed to make the embedded secret message more sensitive to illegal modifications without affecting the property of stego image. To achieve the property of stego image in the various attacks, the robust technique of DWT should be adopted. So how to develop the robust DWT methods for various kinds of media content needs to be further studied.

IV. References

[1] Janki Jasani and Sarita Viswalia, "A Secure and High Capacity image Hiding Scheme Using DWT and Arithmetic Coding", proceeding of the IEEE 3rd International Conference on Computing for Sustainable Global Development, pp.492-496, 2016

[2] Panda SS "A secure approach to spatial image Steganography", VIT University, Vellore, India, pp.13384-13400, 2016.

[3] Lindawatiand Rita Siburian, "Steganography implementation on android Smartphone using the LSB to MP3 and Wav Audio", proceeding of the IEEE 3rd International Conference on Wireless and Telematics, pp.170-174, 2017.

[4] Qi Li, Xin Liao, Guoyong chen and Liping Ding, "A novel game-theoretic model for content-adaptive image Steganography", proceeding of the IEEE 37th International Conference on Distributed Computing Systems Workshops, pp.232-237, 2017.

[5] Narendra Panwar, Dr. Manmohan singh Rauthan and Dr.Amit Agarwal, "Privacy of Patient information", proceeding of the IEEE International Conference on Micro-Electronics and Telecommunication Engineering, pp.232-234, 2016.

[7] Bajwa IS "A new perfect hashing based approach for secure steganograph", 6th International Conference on Digital Information Management", pp.174-178, 2011.

[8] Yasmina M.A. Abdalnour, Ashraf Saad Huwedi and kenz A. Bozed University of Benghazi, "Image Steganography Approach Based on Straight Line Detection",proceeding of the IEEE 17th International conference on Sciences and Techniques of Automatic Control and Computer Engineering", pp.317-327, 2016.

[9] Runtong Zhang, Donghua chen, Xiaopu Shang, Xiaomin Zhu and Kecheng Liu, "A knowledge-Constrained Access Control Model for Protecting Patient Privacy in Hospital Information Systems", proceeding of IEEE Journal of Biomedical and Health Informatics, pp.901-911, 2017

[10]D. Bouslimi, R. Bellafqira and G. Coatrieux, "Data Hiding in Homomorphically Encrypted Medical Images for Verifying Their Reliability in both Encrypted and Spatial Domains", proceeding of the IEEE, pp.2496-2499, 2016.

[11]M. Khodaei, K. Faez, "Adaptive Data Hiding Using Pixel-Value-Differencing and LSB Substitution", Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, pp.1-12, 2016.

[12]Weiming Zhang, Hui Wang, Dongdong Hou and Nenghai Yu, "Reversible data hiding in encrypted images by reversible image transformation", Proceeding of the IEEE Transactions On Multimedia, pp.1-11, 2016.

[13]Aura Conci, Andre Luiz Brazil Simone bacellar Leal Ferreira and Trueman MacHenry, "AES Cryptography in Color
Image Steganography by Genetic Algorithm", proceeding of the IEEE International Conference of Computer Systems and Applications,pp.1-8, 2015.

[14]S. Sriram , B. Karthikeyan , V. Vaithiyanathan and M. M. Anishin Raj, "An Approach of Cryptography and
Steganography using Rotor cipher for secure Transmission", proceeding of the IEEE International Conference on Computational Intelligence and Computing Research, 2015.

[15]Khan farhan Rafat and Muhammad Junaid Hussain, "Secure Steganography for Digital Images" proceeding of the International Journal of Advanced Computer Science and Applications, pp.45-59, 2016.

[16]Tomas Denemark and Jessica Fridrich, "Steganography with Multiple JPEG Images of the Same Scene", proceeding of the IEEE Transactions on Information Forensics and Security, pp.1-13, 2016.

[17]Weixuan Tang, Bin Li, Weiqi Luo and Jiwu Huang, "Clustering steganographic Modification Directions for Color Components", proceeding of the IEEE, pp. 1-11, 2015.

DOI- 10.18486/ijcsnt.2018.7.2.01
ISSN: 2053-6283

[18] Nematollah Zarmehi and Mohammad Ali Akhaee, "Digital video steganalysis toward spread spectrum data hiding" proceeding of the IET Journals, pp.1-8, 2015.

[19] Jiang Yu, Fengyong Li, Hang Cheng and Xinpeng Zhang, "Spatial Steganalysis Using Contrast of Residuals", proceeding of the IEEE", pp.989-992, 2016.

[20] Klimis Ntalianis and Nicolus Tsapatsoulis, "A Robust Video-Object Steganographic Mechanism Over Wireless Networks", proceeding of the IEEE Transactions on Emerging Topics in Computing, pp.1-18,2015

Author's Biography

Mayank Kulshrestha has received the Bachelor of Engineering in Computer Science from Sri Ram College of Engineering and Management, Gwalior. He is currently pursuing his masters (M. Tech) in Cyber Security fromM.I.T.S, Gwalior. He is member of IEEE

.

Manish Dixit, received his B.E. in Computer Technology from Barkatullah University,Bhopal, M.E in Communication Control and Networking from M.I.T.S, Gwalior and PhD .from R.G.T.U, Bhopal. He is currently working as an Associate Professor in the Department of Computer Science and Information Technology, MITS, Gwalior, India. He has presented more than 75 research papers in National and International Conferences and Journals. He is a fellow Member of IETE, senior member of IEEE and Secretary of IEEE MP Subsection. He is member of IET, IAENG and CSI

DOI- 10.18486/ijcsnt.2018.7.2.01
ISSN: 2053-6283