A Survey of State of the Art techniques of Steganography

C. Vanmathi[1], S. Prabu [2]
[1] School of Information Technology and Engineering
[2] School of Computing science and Engineering
VIT University
Vellore, Tamilnadu
India
[1] vanmathi.c@vit.ac.in
[2] sprabu@vit.ac.in

***Abstract*— Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. The main goal of steganography is to ensure that the transmitted message is completely masked, thereby ensuring that the message is accessible only to the intended receiver and not to any intruders or unauthorized parties. In steganography, rather than robustness, the ultimate goal is to hide a message into a cover signal in such a way that an adversary is not even able to understand if the signal contains a hidden message or not. Due to the possible malicious uses of steganography and to the necessity of rigorously assessing the undetectability of the hidden message, steganography is always paralleled by steganalysis, i.e., the set of techniques that an adversary may use to discover the presence of the hidden signal. This review paper discusses about the recent steganography techniques along with their strengths and weaknesses.**

Keyword - Image steganography, payload, stego image, cover image, secret sharing.

I. INTRODUCTION

In modern era of digital communication a transfer of a secret message is a contestable one. Several methods have been proposed and investigated in the literature to provide privacy for communication. Steganography embeds a secret message into images, referred to as cover images, without stimulating attention to individuals. Steganography hides data for various purposes, including secret data storing, confidential communication, and authentication. The main goal of the steganography is to make the secret communication insensible; it conceals the very existence of the secret message [1].

Steganography is applied in various fields and applications like intelligence agencies [2], military agencies [3], medical imagery [4][5], TV broadcasting [6], Checksum embedding [7], advanced data structures [8][9] , radar systems and remote sensing.

In this paper we have provided a review of the state of the art steganography techniques. The paper has been organized as follows: Section 2 describes the different types of steganography techniques. Section 3 reviews recent methods proposed by researchers for strengthening steganography techniques followed by conclusion in Section 4.

I. DISCUSSION OF DIFFERENT STEGANOGRAPHIC TECHNIQUES

The steganography techniques are broadly classified into spatial domain, transform domain, spread spectrum, statistical methods, distortion and cover generation techniques. Spatial domain techniques are also called as substitution techniques. In substitution technique the secret message bits is encoded in the insignificant parts of the cover image. Since there are only minor changes in the image the sender assumes the attacker will not notice the changes in the original image. But it is vulnerable to signal processing attacks and also it loses the total information for lossy compression techniques.

The Transform domain techniques hides the information in significant bits of the cover image hence it is robust to the techniques like compression and cropping. Most common transform domain techniques are discrete cosine transform and wavelet transforms. A trade off exists between the amount of secret information to be embedded and the robustness obtained [10]. Spread spectrum deals either cover image as noise or tries to add pseudo random noise to the cover image.

The next is statistical technique also called as model based technique which modifies the statistical characteristic of the cover image in addition it preserves them in embedding process. [11] This modification can be perceived by humans by identifying the luminance variation. This technique is vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks.

The Distortion technique requires the knowledge of the cover image in the decoding process. In practice it is not efficient method because the secret message can be extracted if the original cover image is available to the

attacker. In earlier days most text based hiding methods were distortion type. The last technique is cover generation; in this the digital cover is generated only for the purpose of being a cover for secret message transfer. Regular expressions and mimic functions are used to generate a cover.

II. SURVEY ON DIFFERENT STEGANOGRAPHIC METHODS

Chia-Chun Wua et al.[12] used spatial domain technique for improving the quality of the image under different payload and authentication bits condition. They used optimal LSB method used by Chan and Cheng. Then they proposed the optimal pixel adjustment process to minimize the embedding error. The embedding error value is given as $\delta i = pi' - pi$ where pi is the pixel value of the cover image before embedding , and pi' is the pixel value of the stego image after embedding the secret bit using normal LSB substitution. To minimize the distortion 2^z is added or subtracted from the embedding pixel value, where z is the total number of embedding bits. The results of the proposed scheme were comparatively better than those of chan and yang et al.

Esra Satir et al. [13] developed a text based steganography to solve the capacity and security issues of the existing method in data compression. They have chosen the frequently used algorithm LZW as a compression method for their proposed scheme and they used stego cover as an email platform. Two secret stego keys are used in embedding process one is global stego key which is a set of email addresses and other is set of modified and chosen email addresses. In the embedding process the final second key value is constructed based on the secret message bits and the text message bits in the original email message based on the proposed algorithm steps. In the decoding phase each element of the first key is compared with the second key value for information extraction. Based on the local complexity of the cover image the embedding capacity of the pixel value is determined. They tested the algorithm using a secret message with length of 300 characters and they achieved 7.042 % improvement compared to existing methods.

Anastasia Ioannidou et al. [14] proposed an algorithm by combining [15] a high payload embedding scheme for color images and [16] a hybrid edge detector for secret message data embedding. Higher peak signal to noise ratio is achieved for the same number of bits per pixel of embedded image. An edge in the image is found by fuzzy edge detector, laplacian filters and sobal edge detector. They achieved better PSNR value but the relationship between the neighboring pixel is not considered into account for data embedding.

V.M. Potdar et al. [17] introduced a spatial domain technique for fingerprinted secret message sharing steganography. The proposed algorithm is robust against image cropping. They divided the secret message into multiple parts and hid each part in the cover medium. They did not concentrate on the embedding algorithm; they have concentrated only on the recovery of the secret message from the cover. The main idea behind their work is that they have used Lagrange interpolating polynomial method and threshold scheme to recover a secret message from the cover. The Computational complexity is high in the proposed method.

Xiaotian Wu et al. [18] proposed a reversible steganography method using the mathematical concept cellular automata. They used 2D reversible cellular automata with memory to encrypt the secret message into shared data. The stego image is obtained by embedding the shared data into the cover image. In the extraction phase the reversible linear concept of memory with the shard data is computed in order to recover the secret image and the original image. This method provides significant imperceptibility to the stego image. They have also provided suggestions for solving the overflow problem in the proposed method. This algorithm can be improved by increasing the shared data to n values instead of t – threshold values.

Fei Peng et al. [19] presented a reversible hiding method based on the integer transform and adaptive embedding. According to the pre estimated distortion the image block is identified. The parameter in integer transform is selected in different blocks which help to embed the secret bits in smooth block rather than sharper ones. Algorithm concentrates on location map and auxiliary information which provides the length of the message and flag bit which identifies the embedding mechanism. This provides a good quality image with high payload capacity. Test results show that the proposed method achieved an additional 2.17 bits per pixel payload than the existing schemes. A tradeoff exits between the capacities of the secret bit embedded per block and the distortion created in the stego image.

Ersin Esen et al. [20] presented a challenging embedding method to hide the secret bits in forbidden zone. The forbidden zone is host signal range where alternations are not allowed. They compared the canonical binning-based data hiding schemes, such as QIM and DC-QIM, empirically, as well as in a theoretical framework. The proposed method uses a masking [21] concept for data hiding. The results of the proposed method shows that it exhibited a better performance compared to DC-QIM and also achieved minimal Watermark to Noise Ratio (WNR).

Dora M et al. [22] introduced a frequency domain technique using an efficient sorting of the wavelet coefficients of the secret messages. Next the Indirect LSB substitution is used for hiding speech signals into speech signals. The proposed Efficient Wavelet Masking (EWM) method follows two principles, the first is the efficient adaptation and the second one is the masking property using threshold criterion. This method ensures efficient coefficient selection of host signal for secret message coefficient and also higher level of perceptual

transparency. This algorithm also reduces the statistics between the host signal and the stego image. They also tested this algorithm with different steganalysis domains like frequency, time and wavelet domain. According to the analysis the EWM is best for low and high capacity data embedding.

Hideki Noda et al. [23] proposed a JPEG steganographic technique for DCT domain using quantization index modulation (QIM) . The J-Steg, F5 and OutGuess are well known popular JPEG steganographic high capacity embedding tools. J-steg can be detected by chi-square attack [24] and the F5 can be detected by a specific technique which efforts the significant change in the histogram of the DCT quantized coefficients stimulated by embedding [25]. They experiments the methods Histogram, quasi preserving JPEG and QIM preserving methods using image processing software. The software produces JPEG compressed bit stream rather than JPEG file. The two methods give high performance in terms of embedding rate, PSNR and histogram preservation. The important and distinct feature is that the embedding is done just during the quantization of DCT coefficients instead of by modifying already quantized coefficients. This allows integrating the extra information using pre round coefficient values from an uncompressed cover image. This is an important issue for further investigation.

X. Li and Wang [26] proposed a steganographic method which modifies the JPEG quantization table and inserts the secret bits in the middle frequency coefficients of the cover image. Secret bits are inserted into Data is inserted into the insignificant bits of DCT coefficients, even though changing any single coefficient value would affect the entire block pixels [27]. Li also proposed another method based on JPEG and Particle Swarm Optimization algorithm (PSO). An optimal substitution matrix is derived for transforming a secret message using PSO algorithm. The standard JPEG quantization table is also modified to occupy more secret messages. The transformed values are hidden in the middle frequency components of the quantized DCT coefficients of the cover-image. The JPEG stego image is generated by using JPEG entropy coding method. The proposed method has high payload, better image quality and security. Raja et al. [29] uses fast Fourier transform methods produces round-off errors, which is not suitable for hidden communication.

Pei-Yu Lin et al. [30] introduced a method which produces a lossless secret message and the original image from the distorted stego images. It uses the (t, n) threshold secret sharing system introduced by Blakley [31] and Shamir [32]. Retrieving original image is especially important in the fields like medical, military. This approach preserves the fidelity of the cover image. The idea behind this method is first transform the secret pixels into m-ary where m value is equal to 7. Then (t-1) secret bits are embedded into F(x) polynomial instead of one secret pixel Lin and Tsai [33], Yang et al.,[34] to increase the payload capacity. The embedding and they also utilized the quantization operation to recover the original image from the cover image. The proposed algorithm calculates the d value as d = p mod m, where m is a prime number and p is the pixels of the cover image (masked pixels). The secret message is converted into (t-1) digits using modulo m representation then F(x) is calculated from (t-1) digits and Q=[p/m] x m. The secret key ki is applied for calculating the hiding data from the secret message. They tested the algorithm with different types of images to estimate the quality of the stego image. They achieved a better PSNR. Smaller the value of m the better is the quality of the stego image, but this reduces the capacity of the secret data to be embedded.

Fangjun Huang et al. [35] presented a new channel selection procedure for JPEG steganography to minimize a detectable distortion. The procedure considers three factors – permutation error, quantization step and the magnitude of the quantized DCT coefficient to be modified. They proved the efficiency of the proposed method by the JPEG Steganalyzers like ClbJFMP, MP, ClbMP and POMM.

Xinpeng Zhang et al. [36] proposed a modified pixel value differencing steganography with higher imperceptibility and larger payload. The proposed method overcomes the disadvantage of pixel value differencing method proposed by Wu and Tasi [37]. Pseudo-random dithering is applied to the division of ranges of the pixel-value differences which effectively handles the vulnerability of histogram analysis.

Xian-ting Zeng et al. [38] presented a method for lossless data hiding with large payload based on histogram shifting and multi layer embedding. The original image and secret information is extracted from the stego image by using only the length of the hidden data, no other extra information is needed. In the proposed scheme 13 layer embedding could be applied and achieved greater than 0.7 bpp compared to existing method.

III. CONCLUSION

This paper briefly describes a survey on recent steganography techniques for image in spatial and transform domain. The strong and weak points of these techniques in general are as follows. The strength of the steganographic technique relies mainly on three factors - imperceptibility level in the stego image, robustness and embedding capacity. The steganographic system leaves unique patterns on the cover images and these patterns feats the steganalyst. The emerging techniques such as DCT, DWT and adaptive steganography are not less prone to steganalysis, especially when the size of the secret message is small. The distortion is also less because embedding is performed in transform domain. So the above problems must be addressed while designing a steganography technique which is robust to attacks.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J.Fridrich, and. Kalker. "*Digital Watermarking and Steganography* (Second Edition)", Morgan Kaufmann Publishers, 2007, ISBN: 978-0-12- 372585-1.

[2] Rebecca T. Mercuri, *The many colors of multimedia security*. Communications of the ACM, , 2004, 47:25-29.

[3] P. Wayner. *Disappearing cryptography*. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition, 2002. ISBN 1-55860-769-2.

[4] R Rodriguez-Colin, F.-U. Claudia, and G. de J. Trinidad-BIas. *Data hiding scheme for medical image*s. In 17th IEEE Inti. Conference on Electronics, Communications and Computers, February 2007 pages 33-38.

[5] Y. Li, C. T. Li, and C. H. Wei. P*rotection of mammograms using blind staganography and watermarking*. In 3rd Inti. Symposium on Information Assurance and Security, August 2007.

[6] N.F. Johnson, S. Jajodia, *Exploring steganography: seeing the unseen*, IEEE Computer 31 (2) (1998) 26–34.

[7] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, *Applications for data hiding*, IBM Systems Journal 39 (3&4) (2000) 547–568.

[8] H. Pang, K. L. Tan, and X. Zhou. *StegFS: a steganographic file system*. In 19th IntI. Conference on Data Engineering, March 2003, pages 657- 667.

[9] S. Hand and T. Roscoe. *Mnemosyne: Peer-to-peer steganographic storage*. In 1st Inti. Workshop on Peer-to-Peer Systems, volume 2 429, , March 2002, pages 130-140.

[10] B. Li, J. He, J. Huang, and Y.Q. Shi, *A survey on image steganography and steganalysis*." Journal of Information Hiding and Multimedia Signal Processing. 2011

[11] S.C. Katzenbeisser. *"Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking*,2000

[12] Chia-Chun Wua, Shang-Juh Kaoa, Min-Shiang Hwangb, *A high quality image sharing with steganography and adaptive authentication scheme*, 2011

[13] Esra Satir , Hakan Isik , *A compression-based text steganography method* , The Journal of Systems and Software 85 (2012) 2385– 2394

[14] Anastasia Ioannidou , Spyros T. Halkidis , George Stephanides , *A novel technique for image steganography based on a high payload method and edge detection*, Expert Systems with Applications 39 (2012) 11517–11524

[15] EL-Emam, Nameer N, *Hiding a large amount of data with high security using steganography algorithm*. Journal of Computer Science, 3(4), (2007),pp 223–232.

[16] Chen, Wen-Jan, Chang, Chin-Chen, & Hoang Ngan Le, T. (2010). *High payload steganography mechanism using hybrid edge detector*. *Expert Systems with Applications*, 37(4), 3292–3301

[17] V.M. Potdar, S. Han, E. Chang, *Fingerprinted secret sharing steganography for robustness against image cropping attacks*, Proceedings of IEEE Third International Conference on Industrial Informatics (TNDIN), Perth, Australia, 10-12 August 2005, pp. 717-724.

[18] Xiaotian Wua,, Duanhao Oua, Qiming Lianga, Wei Sunb , *A user-friendly secret image sharing scheme with reversible steganography based on cellular automata* ,, The Journal of Systems and Software 85 (2012) 1852– 1863

[19] Fei Peng, XiaolongLi, BinYang , *Adaptive reversible data hiding scheme based on integer transform*. Signal Processing (2012) 54–62

[20] Ersin Esen , A. Aydın Alatan , *Comparison of Forbidden Zone Data Hiding and Quantization Index Modulation* ,Digital Signal Processing 22 (2012) 181–189

[21] A.B. Watson, R. Borthwick, M. Taylor, *Image quality and entropy masking, in: Human Vision and Electronic Imaging*, Proc. SPIE 3016 (1997) 2–12.

[22] M. Ballesteros L , Juan M. Moreno A , Highly *transparent steganography model of speech signals using Efficient Wavelet Masking ,Expert Systems with Applications* 39 (2012) 9141–9149

[23] Hideki Noda , Michiharu Niimi , Eiji Kawaguchi, *High-performance JPEG steganography using quantization index modulation in DCT domain* ,Pattern Recognition Letters 27 (2006) 455–461 ,

[24] Westfeld, A, F5—A steganographic algorithm: *High capacity despite better steganalysis*. Lect. Notes Comput. Sci. 2001, 2137, 289–302.

[25] Fridrich, J., Goljan, M., Hogea, D.,. *New methodology for breaking steganographic techniques for JPEGs*. Proc. SPIE 5020, 143–155. 2003

[26] X. Li, J. Wang, A *steganographic method based upon JPEG and particle swarm optimization algorithm*, Information Sciences 177 (15) (2007) 3099-3109l.

[27] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, *A new genetic algorithm approach for secure JPEG steganography*, in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22-23 April 2006, pp. 1-6.

[28] Xiaoxia Li, Jianjun Wang , *A steganographic method based upon JPEG and particle swarm optimization algorithm* ,Information Sciences 177 (2007) 3099–3109

[29] K.B. Raja, C.R Chowdary, K.R Venugopal, L.M. Patnaik, *A secure image steganography using LSB, DCT and compression techniques on raw images*, in: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, 2005, pp. 170-176.

[30] Pei-Yu Lin , Chi-Shiang Chan , *Invertible secret image sharing with steganography ,Pattern Recognition Letters* 31 (2010) 1887–1893 ,

[31] Blakley, G.R., *Safeguarding cryptographic keys*. In: Proc. AFIPS National Computer Conf., 1979, vol. 48, pp. 313–317.

[32] Shamir, A., *How to share a secret. Comm.* ACM 22 (11), 1979, 612–613.

[33] Lin, C.C., Tsai, W.H.,. *Secret image sharing with steganography and authen*tication. J. Syst. Software 73 (3), 2004, 405–414.

[34] Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C. *Improvements of image sharing with steganography and authentication*. J. Syst. Software 80 (7), 2007, 1070–1076.

[35] Fangjun Huang, Jiwu Huang and Yun-Qing Shi, *New Channel Selection Rule for JPEG Steganography* , ,IEEE transactions on information forensics and security , 2002

[36] Xinpeng Zhang , Shuozhong Wang , *Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security*, Pattern Recognition Letters 25 (2004) 331–339 .

[37] Wu, D.C., Tsai, W.H. *A steganographic method for images by pixel-value differencing. Pattern Recognition* Lett. 24, 2003, 1613–1626

[38] Xian-ting Zeng , Zhuo Li , Ling-di Ping , Reversible *data hiding scheme using reference pixel and multi-layer embedding* , International Journal of Electronics and Communications (AEÜ) 66 (2012) 532– 539 .