A Short Survey on Image Steganography and Steganalysis Techniques

Yambem Jina Chanu
Department of Computer Science & Engineering, NERIST,
Nirjuli, Arunachal Pradesh
jina.yambem@gmail.com

ThemrichonTuithung
Department of Computer Science & Engineering, NERIST,
Nirjuli, Arunachal Pradesh
t_tuithung@yahoo.com

Kh. Manglem Singh
Department of Computer Science & Engineering,
NIT Manipur
manglem@gmail.com

Abstract-**The paper describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image. The strong and weak points of these techniques are mentioned briefly so that researchers who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. One can develop a better steganography technique by analyzing the contemporary steganalysis techniques.**

Keywords:- Image steganography, steganalysis, higher order statistic, RS method, spatial domain, transform domain.

I. INTRODUCTION

With advancements in digital communication technology and the growth of computer power and storage, the difficulties in ensuring individuals' privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another. Various methods have been investigated and developed to protect personal privacy. Encryption is probably the most obvious one, and then comes steganography. Encryption lends itself to noise and is generally observed while steganography is not observable. The term steganography refers to the art of covert communications [1]. Steganography's aim is to make the secret communication undetectable, that is, to hide the presence of the secret message. It modifies the carrier in an imperceptible way only so that it reveals nothing neither the embedding of a message nor the embedded message itself. The recent development of the Internet has brought new attention to steganography. The interest in steganography has been enhanced recently by the emergence of commercial espionage and the growing concerns about homeland security due to terrorism. The purpose of steganography is therefore to hide a secret message in a carrier. With the arrival of the digital era and the generalized usage of the Internet and email for the exchange of files, digital covers such as audio, image and video files have become the most obvious choices. This is partly due to their wide spread use, but also because this type of media usually includes a random noise component in which the secret message may be easily hidden. For decades people strove to develop innovative methods for secret communication. A thorough history of steganography can be found in the literature [2-4].

With the boost in computer power, the internet and with the development of digital signal processing, information theory and coding theory, steganography has gone "digital". In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Steganography is employed in various useful applications, such as advanced data structures [5,6], medical imagery [7,8], strong watermarks [9,10], military agencies [9], intelligence agencies [11], document tracking tools [9], document authentication [9], general communication [12], digital elections and electronic money [13], radar systems and remote sensing. Individuals' details are embedded in their photographs in smart IDs and identity cards [14].

The paper is organized as follow. Section 2 describes the different types of steganography techniques. Section 3 gives the different types of steganalysis techniques followed by conclusion in Section 4.

II. TYPES OF STEGANOGRAPHY

Steganography can be either spatial or transform domain. In general, steganographic algorithms rely on the replacement of some noise component of a digital object with a pseudo-random secret message [3]. In spatial domain methods, a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the least significance bits (LSBs). To the human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. It is seen that embedding in the higher LSB generates more visual distortion to the cover image as the hidden information is seen as ''non-natural''. Although LSB embedding methods hide data in such a way that human does not perceive it, these embeddings often can be easily destroyed. As LSB embedding takes place on noise, it is likely to be modified, and destroyed, by further compression, filtering, or a less than perfect format or size conversion. Hence, it is often necessary to employ sophisticated techniques to improve embedding reliability.

Potdar et al. [15] used a spatial domain technique in producing a fingerprinted secret sharing steganography for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub- images and compress and encrypt the secret data. The resulting data is then sub-divided in turn and embedded into those image portions. To recover the data, a Lagrange Interpolating

978-1-4577-0748-3/12/$26.00 © 2012 IEEE

Polynomial was applied along with an encryption algorithm. However, the computational load was high. Shirali-Shahreza and Shirali-Shahreza [16] exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls into the spatial domain if the text is treated as an image.

Colour palette based steganography exploits the smooth ramp transition in colours as indicated in the colour palette. The LSBs here are modified based on their positions in the palette index. Johnson and Jajodia [3] were in favour of using BMP (24 bit) instead of JPEG images. Their next-best choice was GIF files (256-color). BMP as well as GIF based steganography applies LSB techniques, while their resistance to statistical counter- attacks and compression are reported to be weak [4,17-20]. BMP files are bigger compared to other formats, which render them improper for network transmissions. JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain.

Jung and Yoo [21] down-sampled an input image to half of its size and then used a modified interpolation method, termed the neighbor mean interpolation (NMI), to up-sample the result back to its original dimensions ready for embedding. For the embedding process the up-sampled image was divided into 2×2 non-overlapping blocks. Piyu Tsai et al. [22] divided the image into blocks of 5×5, where the residual image is calculated using linear prediction. Then the secret data is embedded into the residual values, followed by block reconstruction. Histogram-based data hiding is another commonly used data hiding scheme. Li et al. [23] propose lossless data hiding using the difference value of adjacent pixels.

Li and Wang [24] presented a steganographic method that modifies the quantization table of JPEG images and inserts the hidden bits in the middle frequency coefficients. Data is inserted into discrete cosine transform (DCT) coefficients' insignificant bits; however, altering any single coefficient would affect the entire block pixels [25]. According to Raja et al. [26] fast Fourier transform (FFT) methods introduce round-off errors; thus it is not suitable for hidden communication. However, Johnson and Jajodia [3], thought differently and included it among the used transformations in steganography. McKeon [27] utilised the 2D discrete Fourier transform (DFT) to generate Fourier based steganography in movies.

Andreas Westfeld based his ''F5'' algorithm [28] on subtraction and matrix encoding (also known as syn- drome coding). F5 embeds only into non-zero AC DCT coefficients by decreasing the absolute value of the coefficient by 1.

III. Types of Steganalysis Techniques

Steganalysis is the art of detecting the existence of hidden information [29,30]. It attempts to defeat the goal of steganography. Steganalysis has its applications in cyber warfare, computer forensics, tracking criminal activities over the Internet and gathering evidence for investigation (particularly in the case of international terrorism). Steganalysis is also practiced for evaluating, identifying the weaknesses, and improving the security of steganographic systems. Some of the recently developed detection methods are explained in this section.

Westfeld and Pfitzmann [31] introduced a statistical analysis method to detect hidden messages. The main idea behind this method is to compare the theoretically expected frequency distribution of the pair of values (PoVs) with the real observed ones. This approach can only detect sequential messages hidden in the first available pixels' LSBs, as it only considers the descriptors' value. It does not take into account that, for different images and the threshold value for detection may be quite distinct . This method provides very reliable results for steganography based on sequential LSB replacement. However, we can only detect randomly scattered messages with this method when the message length becomes comparable with the number of pixels in the image.

Farid et al. [32,33] introduced a higher order statistic method to detect hidden message. This detection method consist of two subsections. The first subsection is extraction, where feature vectors are extracted from the image. The second subsection is classification, where a classification algorithm is used to separate the original image from the stego-image with the help of the feature vectors.

Li Zhi et al. [34] introduced a blind detection known as Gradient-Energy Flipping Rate (GEFR) technique for steganalysis. It analyzes the gradient-energy variation due to the hiding process. It estimates the length of embedded message through the analysis of the variation of the gradient energy resulted from the spatial LSB embedding.

Zhang et al. [35] introduced the difference image histogram method for detecting hidden message. They uses the concept of measuring the weak correlation between successive bit planes to construct a classifier for discriminating between stego-images and cover images.

Dumitrescu et al. [36] proposed a method that is used to detect the existence of hidden messages that are randomly embedded in the LSB plane of natural continuous images. The key of the algorithm is to form some subsets of pixels whose cardinalities change with LSB embedding, and such changes can be precisely quantified for stego-images containing randomly scattered hidden messages.

Fridrich et al. [37] developed a steganographic method for detecting LSB embedding in 24-bit color images, known as the Raw Quick Pairs (RQP) method. It is based on analyzing close pairs of colors created by LSB embedding. It works reasonably well as long as the number of unique colors in the cover image is less than 30 percent of the number of pixels. The RQP method can only provide a rough estimate of the size of the secret message. The result becomes unreliable once the number of unique colors exceeds about 50 percent of the number of pixels. RQP method cannot be applied to gray scale images.

Jena et al. [38] introduced an improved steganographic method for detection based on difference image histogram. It reduces the initial bias and estimates the LSB embedding message ratios by constructing equations with the statistics of difference image histogram. Memon et al. [39] approach based on image quality measures is considered for arriving at the steganographic capacity of LSB based image data hiding techniques.

Fridrich et al. [40] proposed the RS steganalysis. This method makes small alternations to the least significance it plane in an image. It uses these alternations and a discrimination function to classify three types of pixels groups: R, S and U. The counts of he groups reflect the embedding length accurately. This method works very well for the random LSB steganography.

CONCLUSION

The paper describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image in spatial domain. The strong and weak points of these techniques are mentioned briefly so that researches who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. The next plan is to develop a steganography technique that is robust to different types of attacks and the majority of contemporary staganlysis techniques fail to detect the presence of secret messages.

REFERENCES

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

[2] N. Provos and P. Honeyman. Hide and seek: an introduction to steganography. *IEEE Security & Privacy Magazine*, 1:32–44,May 2003.

[3] N.F. Johnson, and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2), pp.26-34.

[4] N. Provos and P. Honeyman, 2003. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*, 01(3), pp.32-44.

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

[6] S. Hand and T. Roscoe. Mnemosyne: Peer-to-peer steganographic storage.In 1st *Intl. Workshop on Peer-to-Peer Systems*, volume 2429, pages 130–140, March 2002.

[7] R. Rodríguez-Colín, F.-U. Claudia, and G. de J. Trinidad-Blas. Data hiding scheme for medical images. In 17th *IEEE Intl. Conference on Electronics,Communications and Computers*, pages 33–38, February 2007.

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

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

[10] F. C. Mintzer, L. E. Boyle, and A. N. Cases. Toward on-line, worldwide access to vatican library materials. *IBM Journal of Research and Development*, 40:139–162,Mar 1996.

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

[12] T. Sharp. An implementation of key-based digital signal steganography. In 4th *Intl.Information Hiding Workshop*, 2001.

[13] A. Pfitzmann. Information hiding terminology. In *Proceedings of the First Intl.Workshop on Information Hiding*, Cambridge, UK, May 1996. Springer–Verlag.

[14] Jain, A.K. & Uludag, U., 2002. Hiding fingerprint minutiae in images. In *Proceedings of Workshop on Automatic Identification Advanced Technologies*. New York, USA, 2002. 7- 8 June. pp.97-102.

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

[16] M.H. Shirali-Shahreza, M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10–12 July 2006, pp. 310–315.

[17] E.T. Lin, E.J. Delp, A review of data hiding in digital images, in: Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS'99, the Society for Imaging Science and Technology, 1999, pp. 274–278.

[18] C.C. Chang, C.Y. Lin, Y.Z. Wang, New image steganographic methods using run-length approach, Information Sciences 176 (22) (2006) 3393–3408.

[19] R.J. Hwang, K.T. Shih, C.H. Kao, T.M. Chang, Lossy compression tolerant steganography, in: Proceedings of the First International Conference on The Human Society and the Internet–Internet Related Socio-Economic Issues, Lecture Notes in Computer Science, 2001, vol. 2105, pp. 427–435.

[20] X. Kong, Z. Wang, X. You, Steganalysis of palette images: attack optimal parity assignment algorithm, in: Proceedings of Fifth IEEE International Conference on Information, Communications and Signal Processing, 06–09 December 2005, pp. 860–864.

[21] K.H. Jung, K.Y. Yoo, Data hiding method using image interpolation, Computer Standards and Interfaces 31 (2) (2009) 465–470.

[22] P. Tsai, Y.C. Hu, H.L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89 (6) (2009) 1129–1143.

[23] Z. Li, X. Chen, X. Pan, X. Zeng, Lossless data hiding scheme based on adjacent pixel difference, in: Proceedings of the International Conference on Computer Engineering and Technology, 2009, pp. 588–592.

[24] X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099–31091.

[25] 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.

[26] 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, ICISIP'05, Bangalore, India, 14–17 December 2005, pp. 170–176.

[27] R.T. McKeon, Strange Fourier steganography in movies, in: Proceed- ings of the IEEE International Conference on Electro/Information Technology (EIT), 17–20 May 2007, pp. 178–182.

[28] A. Westfeld, F5-A steganographic algorithm: high capacity despite better steganalysis, in: Proceedings of Fourth International Work- shop on Information Hiding, Lecture Notes in Computer Science, vol. 2137, Pittsburgh, USA, April 2001, pp. 289–302.

[29] J. Zollner, H. Federrath, H. Klimant, et al., "Modeling the Security of Steganographic Systems", in *2nd Workshop on Information Hiding*, Portland, April 1998, pp. 345-355.

[30] R. Popa. An analysis of steganography techniques. Master's thesis, The "Polytechnic" University of Timisoara, Timisoara, Romênia, 1998.

[31] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Lecture Notes in Computer Science*,1768, pp. 61-75, Springer-Verlag, (Berlin), 2000.

[32] H. Farid. Detecting hidden messages using higher-order statistical models. In *Proceedings of the Intl. Conference on Image Processing*, volume 2, pages 905–908. IEEE,Jun 2002.

[33] S. Lyu and H. Farid. Detecting hidden messages usin ghigher-order statistics and Support vector machines. In Proceedings of the Fifth Intl. Workshop on Information Hiding, pages 340–354, Noordwijk- erhout, The Netherlands, 2002. Springer-Verlag.

[34] L. Zhi, S. A. Fen and Y. Y. Xian, " A LSB steganography detection algorithm", Proc. IEEE ISPIMRC, pp. 2780-2783, 2003

[35] T.Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference histogram", Proc. IEEE ISCASS, vol. 3,pp.545-548, 2003.

[36] S.Dumitrescu, X. Wu, and Z.Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE Trans on Signal Proc., vol.51, no.7,Jul. 2003.

[37] J.Fridrich, R.Du, and L.Meng, "Steganalysis of LSB Encoding in Color Images," *Proc. IEEE int'l Conf. Multimedia and Expo,* CD-ROM, IEEE Press,Piscataway, N.J.,2000.

[38] S. K. Jena and G.V.V. Krishna,"Blind Steganalysis of Hidden Message Length,"*Int'l Journal of Computers,Communications and Control*, vol.2, no.2, pp.149-158.

[39] N. Menon, I. Avcibas. and B. Sankur, 'Steganalysis using Image Quality Metrics', SPIE Security and Watermarking of Multimedia Contents Electronic Imaging, San Jose, CA. Statistical Steganalysis, 2001.

[40] J. Fridrich, M. Goljan, and R.Du, " Reliable detection of LSB steganography in color and gray-scale images," Proc. ACM Workshop Multimedia Security, Oct.5, pp.27-30, 2001.