A Comprehensive Review on Secure Image Steganography

Kritika Singla, Sumeet Kaur
Yadavindra College of Engineering, Punjabi University, Patiala
kritikasingla23@gmail.com, Purbasumeet@yahoo.co.in

Abstract: *Steganography is an art and science of hiding secret information within the other information. Different carrier file formats can be used, but digital images are the most popular to hide secret information because the slight modification in the cover image is hard to distinguish by human visual system. In this paper, we are reviewing various steganographic techniques of hiding text in images using image steganography. This paper provides base to researchers who are new in the field of information hiding.*

Keywords: Cover image, Embedding, Extraction, Steganography, Secret message

I. Introduction: Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected.

© *2012 Journal Anu Books* Authors are responsible for any plagiarism issues.

If the message is also encrypted then it provides another layer of protection [1]. Some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover [2]. In the fields of information hiding, there is a visual requirements model, which is called magic triangle, given in Fig. 1 (Johnson, Duric, & Jajodia, 2001). The first requirement, called capacity or also embedding payload, is determined by the number of secret bits embedded in each cover pixel. A higher capacity allows much more the secret data to be inserted into the cover image. The second requirement, named imperceptibility, is usually calculated by peak signal-to-noise ratio (PSNR). When the difference between the cover image and the stego image is small, the PSNR value is high. Thus, the stego image quality is considered to be good with the imperceptibility is high. The last requirement called robustness which prevents the secret data from being attacked or stolen [3].

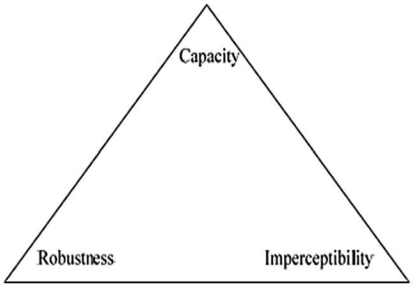

Fig. 1. Magic triangle-three requirements model.

Image steganography takes an advantage of limited power of human visual system. Here unlike watermarks which embed added information in

every part of the image, only the complex parts of the image holds added information [4]. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention [5]. Steganography can also be used in the non-commercial sector to keep private digital information protected for number of purposes such as secret data hiding, copyright protection. Data authentication, ensuring authenticated data availability for academic usage, monitoring of data piracy, labeling electronic data/contents, ownership identification, providing confidentiality and integrity enhancement control of electronic data piracy etc [3]

II. Secure Image Steganography

As described earlier, Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. Image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other mages, or anything that can be embedded in a bit stream can be hidden in an image. The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. This results in the production of what is called a stego-image.

In this section, we are presenting some of the research work of the prominent authors in this field and will be giving various ways in which secure image steganography is done**.**

A. Rubata Riasat, et al, "A hash based approach for color image steganography", 2011 [7] proposed a hash based approach for image steganography. The most important part of the proposed algorithm is the used hashing technique that is perfect hashing. Perfect hashing is faster

© 2012 Journal Anu Books Authors are responsible for any plagiarism issues.

than the other techniques and it reduces hash collision. The proposed approach hides the text to red, green and blue channel of the pixels of the color image by replacing the ASCII value of the first, second and third character with the value of red, green and blue channel respectively. The strong point of the given approach is that it is fast and secure and the weak point of this approach is that picture quality of the output image is not very good.

B. Joyshree Nath, Asoke Nath, "Advanced Steganography Algorithm using Encrypted secret message", 2011 [8] proposed a randomization method for generating the randomized key to encrypt and decrypt the text file. In this work author have used two methods first, in which they encrypt the secret message using a method MSA proposed by Nath et al.(9) and second, in which they insert encrypted secret message inside the cover file by changing the least significant bit(LSB). The strong point of the given approach is that we can embed almost any type of file inside some cover file like image file (.jpeg or .bmp) or any image file inside another image file. Another strong point of the given approach is that if we change the key little bit then the whole encryption and decryption process will change.

C. Amin Milani Fard, et al, "A new genetic algorithm approach for secure jpeg steganography" 2006 [10] proposed a novel genetic algorithm evolutionary process to make secure steganographic embedding on jpeg images. In this work author have proposed a new genetic algorithm approach to find the best position for data embedding and also optimize the quality of the steganographic image. This approach is based upon the Outguess algorithm and the combination of Outguess algorithm and Maximum absolute difference for the image quality are used as GA fitness function. The strong

© *2012 Journal Anu Books* Authors are responsible for any plagiarism issues.

point of the given approach is that it is supposed to defeat all known steganalysis methods.

D. Alaa Taqa, A.A.Zaidan, B.B.Zaidan, "New framework for high secure data hidden in the MPEG using AES encryption algorithm", 2009 [11] proposed a combine approach between cryptography and steganography. In this work Secret key steganography and AES (Advanced Encryption Standard) method is used for secure data hidden inside the digital video as the separate frames. The strong point of the given approach is that secure and large amount of data can be hidden.

E. Kirti Upreti, Kriti Verma, Anita Sahoo, "Variable bits secure system for color images", 2010 [12] proposed a variable length bits embedding in RGB color channels of the colored image. In this work the secret message is converted into two types of the plain texts by subsequent ASCII and binary conversions and the two cipher texts generated by using RSA and IDEA algorithms. This approach is the idea in image steganography, where variable number of bits of encrypted data can be stored in Data channel and their number in Indicator channel and the use of both channels ensure minimum distortion. The strong point of the given approach is that this leads to a very high capacity with minimal distortions.

F. Subba Rao Y.V, Brahmananda Rao S.S, Rukma Rekha N, "Secure image steganography based on randomized sequence of cipher bits" 2011 [13] proposed the randomization of cipher bits for secured image steganography. In this work author generate the random sequences of cipher bits by the use of an L.F.S.R (Linear Feedback Shift Register) and select the random sequence closest to the image and then embed these random sequences of cipher bits in the image. The strong point of the given approach is that there is no one to one mapping between a cipher text and an image.

© 2012 Journal Anu Books Authors are responsible for any plagiarism issues.

The weak point of the given approach is that this cannot hide large data in single image.

G. Sos S.agaian, Ravindranath C.cherukuri, Ronnie sifuentes, "A new secure adaptive steganographic algorithm using Fibonacci numbers", 2006 [14] proposed the algorithm based on Fibonacci bit-plane decomposition and T-order statistics. In this work the T-order statistics enables the embedding of secret data in noisy portions of an image and the Fibonacci bit-plane decomposition enables the decomposition of an image based on Fibonacci numbers creates a higher number of bit planes. The strong point of the given approach is that it enhances the capacity of the secret data to embed.

H. Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", 2010 [15] proposed a steganography scheme which is based on the LSB (least significant bit) steganography mechanism and a hybrid edge detector which combines the fuzzy edge detector with canny edge detector. In this work the hybrid edge detector is applied first on the cover image and then the secret message is embedded in the edges of the image using LSB technique. The strong point of the given approach is that it produces the better quality stego image. The weak point of the given approach is that the capacity is limited according to the edges of the cover image.

I. Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RGB intensity based variable bits image steganography", 2008 [16] proposed an algorithm for RGB image steganography, where the values of R, G and B are used to decide the number of bits to store in each pixel. In this work one of the three channels is used as the indicator and data is stored in one of the two channels other than indicator. lower color component can store

© *2012 Journal Anu Books* Authors are responsible for any plagiarism issues. JAB

higher number of bits because the idea is that, lower color value of a channel has less effect on overall color of the pixel than the higher value. The strong point of the given approach is that it offers very high capacity for cover media compared to existing algorithms.

J. K. Pramitha, Dr. L. Padma Suresh, K. L. Shunmuganathan, "Image steganography using mod-4 embedding algorithm based on image contrast", 2011 [17] proposed a new image steganography method based on image contrast for gray scale images. In this work a group of 2x2 blocks of spatially adjacent pixels is selected as the valid block for embedding the secret message and then modulo 4 operation is applied on each valid block to embed the binary bits. Each secret message is also encrypted by RSA encryption algorithm for more security. The strong point of the given approach is that it increases capacity of the secret data to be hide and provide imperceptible stego image quality.

III. Conclusion

The purpose of this paper is not to present an exhaustive list of variations of each method, rather, it is intended to present a number of secure steganographic approaches that are available. Security is not entirely depends upon strength of cryptographic algorithm, rather, it depends on the secret key which we share with the communicating party.

IV. References

1. A.A.Zaidan et. Al, "Implementation Stage for High Securing Cover- File of Hidden Data Using Computation between Cryptography and Steganography". International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Volume 20, 2009, Manila, Philippines.

© 2012 Journal Anu Books Authors are responsible for any plagiarism issues.

2. B.B Zaidan, et al, “Quality of Image vs. Quantity of Data Hidden in the Image”, International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV’09), 2009, Las Vigas, USA

3. U. Gopinathan, D.S. Monaghan, T.I Naughton, IT. Sheridan, and B. Javidi, “Strengths and weaknesses of optical encryption algorithms,” in Proc. 18th Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2005, 22-28 Oct pp. 951-952

4. Sellars D., “An Introduction to Steganography”,

   cs.uct.ac.za/courses/CS400W/NIS/papers99/ dsellars/stego.html.

5. K. Usman, H. Juzoji, I. NakajiIm, S. Soegidjoko, M. Ramdhani, T. Hori, and S. Igi, “Medical image encryption based on pixel arrangement and random permutation for transmission security,” in Proceedings of IEEE 9th International Conference on e-Health Networking, Application and Services, Taipei, Taiwan, 2007, 19-22 June. Pp.244-247.

6. U. Gopinathan, D.S. Monaghan, T.I Naughton, IT. Sheridan, and B. Javidi, “Strengths and weaknesses of optical encryption algorithms,” in Proc. 18th Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2005, 22-28 Oct pp. 951-952

7. Rubata Riasat, et al, “A hash based approach for color image steganography”, IEEE, 978-1-61284-941-vol-6,2011

8. Joyshree Nath, Asoke Nath, “Advanced Steganography Algorithm using Encrypted secret message”, International journal of advanced computer science and applications, vol2, no. 3, march 2011.

9. A.Nath, S.Ghosh, M.A.Mallik, “Symmetric key cryptography using random key generator”, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2, P-239-244.

© *2012 Journal Anu Books* Authors are responsible for any plagiarism issues.

10. Amin Milani Fard,et al, “A new genetic algorithm approach for secure jpeg steganography”, IEEE transactions, 1-4244-0457-vol-6,2006

11. Alaa Taqa, A.A.Zaidan, B.B.Zaidan, “New framework for high secure data hidden in the MPEG using AES encryption algorithm”, International Journal of Computer and Electrical Engineering, Vol. 1, No. 5 December, 2009,1793-8163.

12. Kirti Upreti, Kriti Verma, Anita Sahoo, “Variable bits secure system for color images”, International conference on advances in computing, control and telecommunication technologies, 2010.

13. Subba Rao Y.V, Brahmananda Rao S.S, Rukma Rekha N, “Secure image steganography based on randomized sequence of cipher bits”, IEEE transactions, 978-0-7695-4367-vol-3, 2011.

14. Sos S.agaian, Ravindranath C.cherukuri, Ronnie sifuentes, “A new secure adaptive steganographic algorithm using Fibonacci numbers”, IEEE, 1-4244-0359-vol-6, 2006.

15. Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, “High payload steganography mechanism using hybrid edge detector”, Expert Systems with Applications 37 (2010) 3292–3301, ELSEVIER.

16. Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub**, “**RGB intensity based variable bits image steganography”, IEEE, 978-0-7695-3473-vol-2, 2008.

17. K. Pramitha, Dr. L. Padma Suresh, K. L. Shunmuganathan, “Image steganography using mod-4 embedding algorithm based on image contrast”, IEEE, 978-1-61284-653-vol-8, 2011.

* * * * *

© 2012 Journal Anu Books Authors are responsible for any plagiarism issues.