International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Image Hiding Steganography with Digital Signature Framework

*** Rajkumari**
M.Tech Student Computer Science and Engineering Dept of CSA Ch. Devi Lal University, Sirsa(Haryana)
Rajkumarisirsa@gmail.com

**** Dr. Raghuvinder Bhardwaj**
Assistant Professor Dept of CSA Ch. Devi Lal University, Sirsa(Haryana)
Raghuvinder.bhardwaj@gmail.com

Abstract:

Data hiding may be a powerful idea in pc security that facilitates the secure transmission data over insecure channel by concealing the initial information into another cover media, Where as text information concealing is kind of a development in computer security applications, image concealing is gaining speedy popularity due to its prevailing applications as a picture is a lot of controlling to contain helpful info. during this paper, we've got carefully investigated the idea of Steganography by incorporating image hiding among another image with a secure structural digital signature framework. Our projected work includes the initial image preprocessing tasks through filtering of the host image followed by embedding of the key image and outline of the image information among the host image. Later, the stego image is given as associate degree input to the digital signature framework by that we will ensure the secure, authentic and error-free transmission over wireless channel of our secret information. The promising experimental results recommend the potential of this framework.

Keywords: Steanography; Data hiding; MSE; PSNR value; Digital signature

1. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words stegano meaning "covered or protected", and graphy meaning "writing". A steganography technique that uses images as the cover media is called an image steganography. The applications of using steganography concept for hiding images play an important role in several fields such as military or intelligence for setting communications between the concerned agents. In the mentioned fields, the transmission of secure messages in terms of images is very frequent. The purpose of using steganography in this perspective is to avoid unwanted attention to the transmission of the secret information [1][3]. The procedure of steganoraphy includes embedding the secret message in a cover media such as image, video, audio, text etc. with a secret key and the extraction of the original secret message at the other end after the transmission is complete [2][3]. The secret message is the information that we intend to hide for avoiding unnecessary manipulation by third parties during transmission.

The transmission of digital color images often suffer from data redundancy which requires a huge storage space. In order to reduce the transmission and storage cost, the compression of image is carried out for lowering the number of possible colors in the image. This, in turn, reduces the image size to a greater extent. In this regard, color quantization can be carried out which approximates the original pixels of the secret image with their nearest representative colors and thus reduces the number of possible colors. This approximation intent to keep the image

International Journal of Research
IJR
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

quality as much as possible so that the visual similarity between the original and the optimized image is kept [5].

2. Image Steganography

A steganography technique that uses images as the cover media is called an image steganography. Hiding secret messages in digital images is the most widely used method as it can take advantage of the limited power of the human visual system (HVS) and also because images have a large amount of redundant information that can be used to hide a secret message.

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels. The individual pixels can be represented by their optical higher frequency side of the visual spectrum. A picture can be represented by a characteristics like brightness, chroma etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s [7].

2.1 Image Steganography Classifications

Generally image steganography is categorized in following aspects [8]

High Capacity: Maximum size of information can be embedded into image.

Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.

Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.

Temper Resistance: It should be difficult to alter the message once it has been embedded into stego-image.

3. Least Significant Bit Substitution

LSB Coding the simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value. If it is using 24-bit color, the amount of change will be minimal and indiscernible to the human eye [17].

4. DIGITAL SIGNATURE

The concept of digital signature is very fascinating in a sense that it authenticates the sender and also checks for the accuracy of the transmitted data. The robust nature of digital signature is contributing to a great extent in applications of computer security related tasks [19]. The concept of structure-based image authentication arises from the increasing need for trustworthy digital multimedia data in various fields such as commerce, industry, defense, etc. Images became popular in the past few years partly because of their efficiency of manipulation. An Editing or modifying the content of a digital image can be done easily with huge efficiency which is not desirable at all while performing secure transmission. To ensure the credibility and trustworthiness, structure-based image authentication techniques are needed for verifying the originality of image content and preventing forgery [20]. SDS is a signature that can be used to determine if a modification done on the output is incidental or malicious. If the content of the image structure is not corrupted, then the modification is believed to be as incidental. Otherwise, it is malicious. This technique is particularly useful in security applications and therefore, we were highly motivated to incorporate the concept in our proposed framework [5].

4. PROPOSED FRAMEWORK

The whole work is divided into two levels. Level 1 is steganography technique in which stego image is being inserted into the cover image using LSB method. Level 2 of security is applying a digital signature over the encrypted image.

1. SI-Stego image
2. CI 1-Cover image 1
3. Hide stego image into Cover image 1 using LSB method which is modified by the author. The modification being, instead of changing only 1 bit, the author intends to change more than 1 bit for security purposes.
4. Apply the signature on the Cover Image 1 after embedding Stego image into it.
5. CI 2-Cover Image 2
6. Now, cover image 1 will act as stego image for cover image 2. This is level 3 of security. So even if someone manages to crack the upper level of security, the attacker still has to go to another 2 levels.
7. This will now the final Cover image to transmit.

After the transmission is over, we authenticated the sender identity by our

8. At the receiver end, we will receive cover image 2
9. Apply the reverse LSB on cover image 2 to obtain cover image 1
10. Apply the signature on cover image 1 to obtain cover image with stego image
11. Again apply reverse LSB on cover image 1 to obtain the stego image.

4. EXPERIMENTAL RESULTS

In this section, we present our preliminary experiments on some digital color images. We will investigate the performance of our proposed framework. To perform the comparison is the use of peak signal-to-noise ratio (PSNR) and MSE. These results are proof that the algorithm shows promising results. And message was properly hidden inside covers and changes are not visible with naked eyes.

digital signature and extracted the secret image from the received stego image.

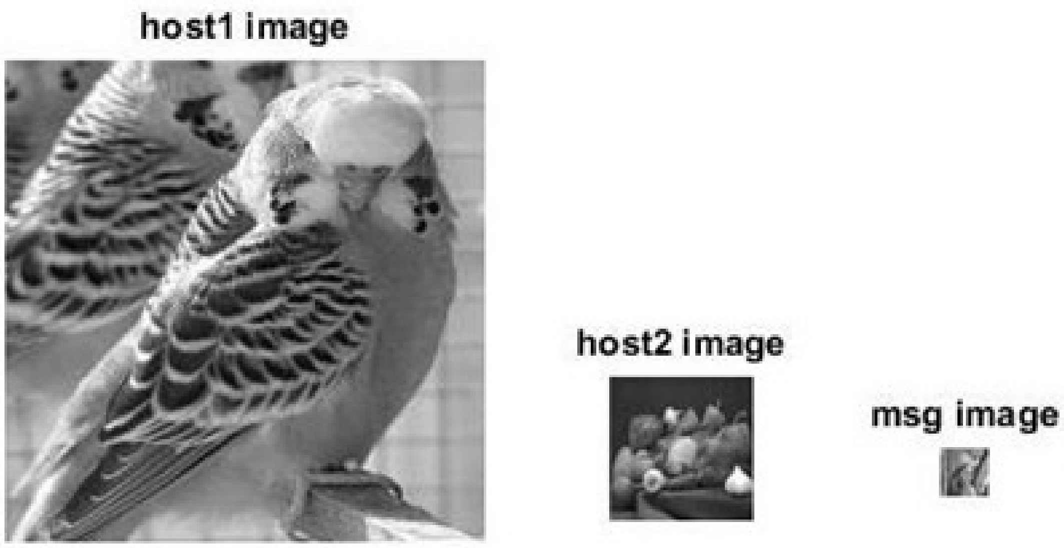

Figure1: Input images

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

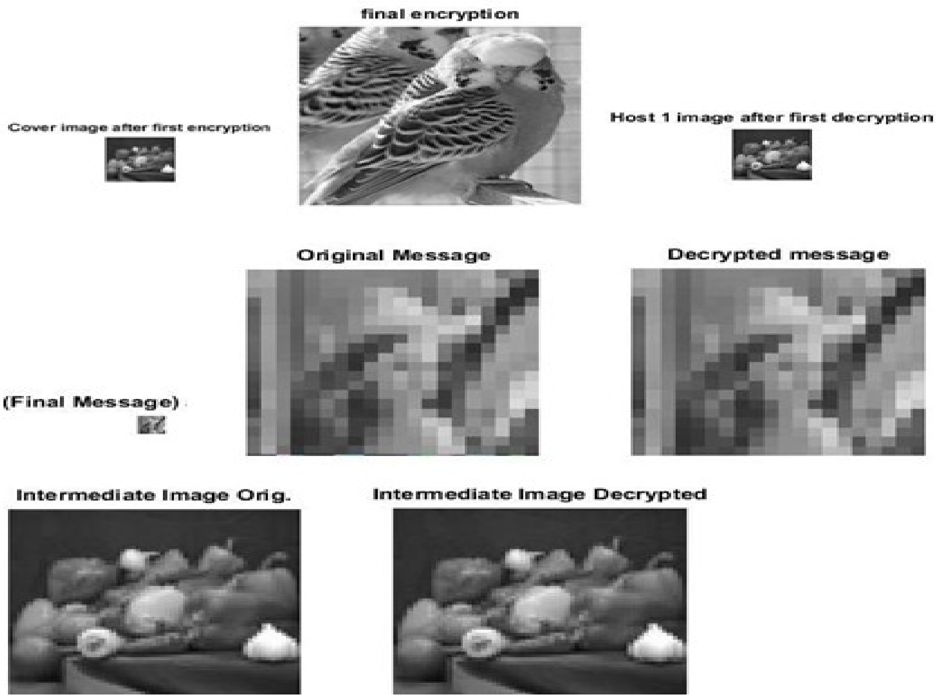

Figure2: After Steganography perform

Table1: Comparison between two host image and message images

Host 1	Host 2	Message Image	MSE	PSNR value	Method in [3]
Bird	Peppers	Lena	40.4877	43.1618	38.67
Cameraman	Lena	Peppers	44.529	44.0736	38.04
Cameraman	Butterfly	Bird	44.8244	44.7875	38.57
coffeepot	Butterfly	Camera man	42.4269	44.7858	38.98

5. Conclusion

Least siginificant bit (LSB) algorithm is used for security purpose and it is used for level one security. On the basis of the study we provide one more level to security. In this, the message image was properly hidden inside cover image 1, and then on a second level, that cover image was again hidden well inside another cover image. After words, we conclude that the level of security is improved by applying the LSB and digital signature.

Hence in order to reach to the message image, we have to undergo 2 level of decryption process. So it very difficult for anyone without the signature key to get that information. Hence, we could easily conclude that given algorithm proves to be working well.

REFERENCES

[1] N. Johnson, "Survey of Steganography software," Tech. Rep., January 2002.

[2]C.J,"Steganography,"http://www.webopedia.com/TERM/S/steganography.html, 2005.

[3] P. Wayner, Disappearing Cryptography: Information Hiding: Steganography and Watermarking (2nd Edition), 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.

[4] Kriti Saroha, P. K. (Volume 11– No.6, December 2010). A Variant of LSB Steganography for Hiding Images in Audio. International Journal of Computer Applications (0975 – 8887) , 5.

[5] Fahim Irfan Alam, M. M. (2013). An Investigation into Image Hiding Steganography with Digital Signature Framework. International journal of Recent trends in engineering , 6.

[6] Prof. Brinda K, P. S. (Volume 3, Issue 11, November 2013). Steganography: Secret Transmission of Data. International Journal of Advanced Research in Computer Science and Software Engineering , 3.

[7] Vijay Kumar Sharma, V. S. (15th February 2012. Vol. 36 No.1). A Salgorithm for hiding Image in image by improved LSB Substitution by Minimize detection. Journal of Theoretical and Applied Information Technology , 8.

[8] E Lin, E Delp, A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, (1999).

[9] A. Joseph Raphael, Dr. V. Sundaram, Head & Director(Vol2 (3)) Cryptography and Steganography – A Survey, A.Joseph Raphael, Dr.V Sundaram, Int. J. Comp. Tech. Appl.

[10] C.Brainos., A. (n.d.). A Study of steganography and the art of hiding information.

[11] Queirolo, F. (n.d.). Steganography in images.

[12] Niels Provos, P. H. (2003). Hide and Seek: Introduction to Steganography.

[13] T. Morkel 1, J. E. (n.d.). An overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group , 12.

[14] Saraireh, S. (Vol.5, No.3, May 2013). A Secure data Communication System using Cryptography and Steganography. International Journal of Computer Networks & Communications (IJCNC) , 13.

[15] Masoud Nosrati, R. K. (august 2011). An introduction to steganography methods. World Applied Programming, Vol (1), No (3) , 5.

[16] Shaveta Mahajan, A. S. (Volume 2, Issue 10, October 2012). A Review of Methods and Approach for Secure Stegnography. International Journal of Advanced Research in Computer Science and Software Engineering , 4.

[17] Maninder Singh Rana, B. S. (Volume1 Issue 1 Oct 2012 Page No. 11-22). Art of Hiding: An Introduction to Steganography. International Journal Of Engineering And Computer Science , 13.

[18] Hussain, M. H. (Vol. 54, May, 2013). A Survey of Image Steganography Techniques. International Journal of Advanced Science and Technology , 12.

[19] M. Murty, D.Veeraiah, and A. Rao, "Digital signature and watermark methods for image authentication using cryptography analysis," Signal & Image Processing : An International Journal (SIPIJ), vol. 2, no. 2, pp. 170–179, June 2011.

[20] D. Bearman and J. Trant, "Authenticity of digital resources: Towards a statement of requirements in the research process," D-Lib Magazine, June 1998.

[21] Falkowski, B. J. (n.d.). Lossless binary image compression using logic functions and spectra.

[22] Ms. Priyanka P. Palsaniya, 2. P. (Volume 3, Issue 2, February 2014). CryptoSteganography:Security Enhancement by

using Efficient Data Hiding Techniques. International Journal of Application or Innovation in Engineering & Management (IJAIEM) , 5.

[23] Al-Hazaimeh, O. M. (Vol. 9, Issue 4, No 2, July 2012). Hiding Data in Images Using New Random Technique. IJCSI International Journal of Computer Science Issues , 5.

[24] C.P.Sumathi, T. a. (Vol.4, No.6, December 2013). A Study of Various Steganographic Techniques Used for Information Hiding. International Journal of Computer Science & Engineering Survey (IJCSES) , 17.

[25] Gabriel Macharia Kamau, S. K. (n.d.). An enhanced Least Significant Bit Steganographic Method for Information Hiding".

[26] Hemachandran, S. A. (2013). Steganography Based On Random Pixel Selection For Efficient Data Hiding. International Journal of Computer Engineering and Technology Vol.4, Issue 2, pp.31-44 , 17.

[27] Jaishree Singh, D. J. (Vol. 4 (3) , 2013, 522-525). Secure Data Transmission using Encrypted Secret Message. Jaishree Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies , 4.

[28] Kuan, R. I. (February 25, 2011.). Steganography Algorithm to Hide Secret Message inside. Computer Technology and Application , 7.