Comparative Analysis of PSNR Value of Image Steganography using LSB Technique

Khusboo Mishra[1], Ramayan pratap singh[2]

[1]M.Tech Scholar, [2]Assistant Professor
Department of Electronics and Communication, VITS, Satna,

***Abstract*: In This Paper, we show you a new digital steganography, entitled spread spread spectrum image steganography (SSIS). Steganography, which means "to write overshadowed" in Greek, is a communicative science. Following the steganography discussion of theory of the consultation and review of existing strategies, the new method, the SSIS, is established. This program hides and returns a broader message within the digital photo while keeping the original size of the image and the dynamic width. Encrypted message can be restored using the appropriate keys without the original image information. Image restoration, copying error management, and techniques such as distribution of spectrum are described, and performance is shown. This message combines this can be text, photo, or any other digital signal. Applications for this encryption application include bandwidth, covert connectivity, image verification, verification, control entries, and tracking.**

***Keywords*: digital steganography, digital photo, Encrypted message, image verification**

1. Introduction

In today's highly competitive and dynamic world, the data and information that feeds the motor of information communications and the global economy. By stimulating the power of the computer, the Internet and the development of digital signal processing (DSP), steganography has become "digital" (Sharma and Shrivastava, 2012). To ensure that data is secured and does not reach unintended destinations, the concept of hiding data has led researchers to come up with creative solutions to protect certain information from failing to fit in the wrong hands (Abraham and Paprzycki, 2004). This idea of hiding data is not a novelty, it has been used over the centuries throughout the world in various regimes, which is a tool to conceal information so it does not even seem to exist (Pavani et.al., 2013). Over the last decade, methods, techniques, and technologies to hide digital evidence and to communicate in secret have grown alarmingly (Hosmer, 2006). Thus, people have adapted different means of hiding information.

A steganographic system involves two parts: the sender embodying the secret message in the coverage environment and the receiver that extracts the message from the cover. The sender receives the object "host," which is the object of coverage and incorporates a secret binary message that produces a stego object that is perceptually identical to the cover. The stego object is then communicated along a public channel to the receiver. At the receiver, the stego object is used to retrieve the secret binary message. The public channel can be monitored by an active supervisor whose purpose is to detect the presence of any hidden communication that takes place. The key (k) is optional because it can be included in the embedding process. The key is specific to the steganography algorithm that ensures that only the recipient who knows the appropriate the extraction key can decode the message from a stego image.

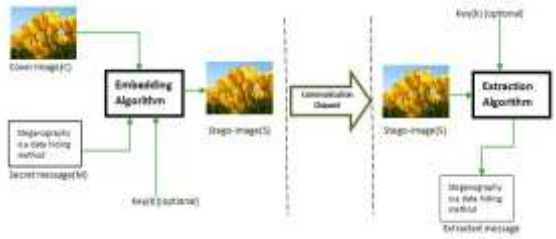

Figure 1.1: The working model of the image steganography system

A steganographic system scenario is shown in Figure 1.1. If a sender wants to send the secret message M to a recipient along the unsafe communication line, the sender incorporates a secret message (M) in the cover (C) by an embedding method to produce stego images (S). The K (optional) key can be used to find the location in C to hide the message. Then the stego-image (S) is sent to the recipient. On receipt, the recipient uses the extraction algorithm to retrieve M (extracted message).

2. Review of Literature

Digital images are the most commonly used environment for steganography, as they are most widely available on the Internet and on the Web. Steganography hides information in the image as multimedia carriers in such a way that it does not attract the attention between billions of images on the internet (Chandramouli et.al 2004). Therefore, steganography of the image is a potential for various communication applications to improve communication security and has become a popular topic in research. The paper in this thesis is related to steganography in image files. This chapter provides a literary analysis of image-based steganography techniques and studies the methods proposed by various authors.

As this thesis focuses on the steganographic technique, first of all the requirements of a basic steganographic system are described. The three most important requirements to be met for steganographic technique are capacity, security and robustness, as in Figure 2.1 (Wang and Wang, 2004). The evaluation of the steganographic technique is done with these

three parameters and there must be compromises between these parameters in order to have a better steganographic technique (Fridrich, 1999b).

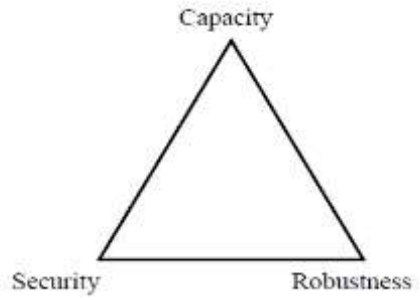

Figure 2.1: Basic requirements of a steganographic system

• Capacity: Capacity refers to the amount of secret information that can be incorporated into the coating environment (Katzenbeisser and Petitolas, 2000). Steganography targets hidden communication and therefore usually requires sufficient integration capacity (Wang and Wang, 2004). Steganographic capacity is the maximum number of bits that can be embedded in a given coverage file without affecting the quality of the shell environment and also minimizing the perception of hidden data in the stego environment. The capacity of the secret message to be embedded must be less than the size of the shell.

Robustness: Robustness is the ability to retrieve hidden information after regular image processing, and embedded data remain intact if the stego medium suffers stego attacks (Frederick, 1999b). The robustness requirement is required when dealing with the ability to conceal data. In steganography robustness is not a top priority, so steganographic systems are not robust against changes or have limited robustness against technical changes (Wang and Wang, 2004).

Security: Security indicates the listener's inability to detect embedded information. This information cannot be removed beyond reliable detection by targeted attacks based on the complete knowledge of the embedding algorithm and the hidden message carrier (Fridrich, 1999b). In order to avoid raising suspicion of attackers, hidden content must be invisible both perceptually and statistically (Wang and Wang, 2004). Therefore, the features and attributes of the cover files need not be changed and distortions must not occur during the integration process (Venkatraman et al., 2004).

The review of digital imaging steganography in this chapter is categorized into two categories:

Steganography in the spatial image domain.

2.2 Steganography in the field of image frequency.

Steganography in the Image Spatial Domain

Steganographic techniques that modify the coverage image in the space domain are known as spatial domain methods involving LSB coding (Sharda and Budhiraja, 2013). The common part of spatial steganography is the direct change of image pixel values to hide data (Li et al., 2011). The basic concept of least significant bit replacement includes the incorporation of secret data into bits that have minimal weights so as not to affect the original pixel value (Kanzariya and Nimavat, 2013). In this method, the least significant bits of some or all of the bytes inside an image are replaced with bits of the secret message, and such approach has become the basis of many techniques that conceal messages from the multimedia carrier data (Pavaniet al., 2013). By changing the RGB of each pixel slightly, a new color is produced that is so close to the original that the difference cannot be visualized and the binary data can be easily hidden in the LSB values of any colored color image (Hosmer, 2006). The LSB-based steganography method either changes the pixel value by ± 1 or leaves it unchanged, which depends on the nature of the hidden bit and the LSB of the corresponding pixel value (Chandramouli and Memon, 2001).

Extraction Algorithm

i. Open the Stego image, read the RGB color of each pixel.

Draw the red pixel plane of the stego image.

ii. Initialize the message bits key in the random red pixel plane where the secret bits are embedded.

iii. For decoding, select the pixels using the same pseudo-random sequence. Since the key knows the k seeds, the kican is rebuilt and hence the entire pixel yi sequence.

iv. Read the LSB of the red plane of each pixel and put it directly into a matrix.

v. Repeat step for the entire pixel index sequence.

Then, the matrix content is converted to decimal, which is actually the ASCII value of the hidden character.

Result and Discussion

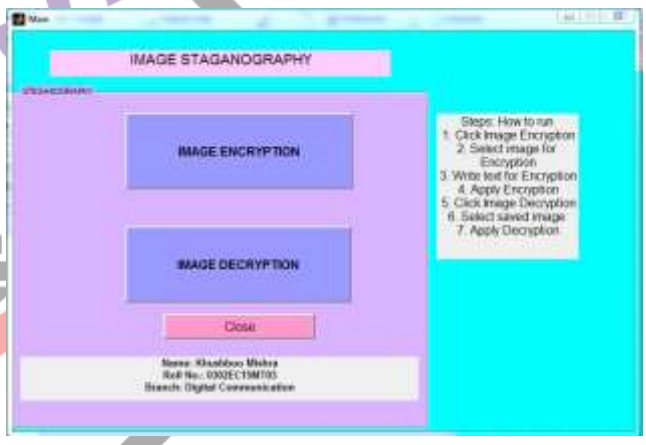

Fig: Basic Layout of Proposed Algorithms using MatLab

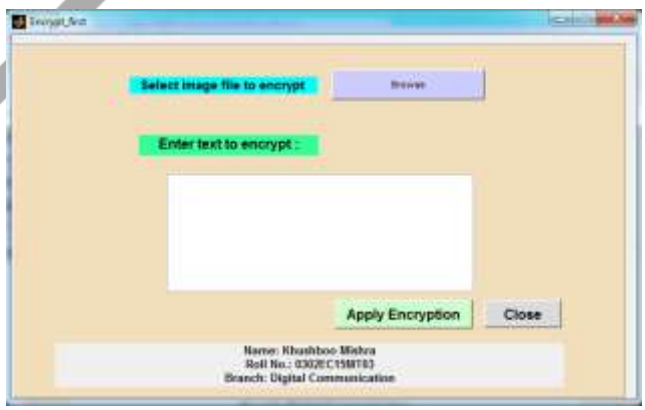

Fig: Image Encryption Basic layout using MatLab

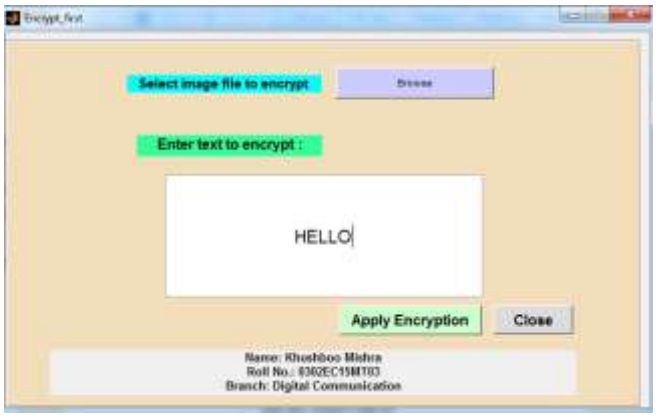

Fig: Select Image File and insert text in image using Image Encryption Basic layout using MatLab

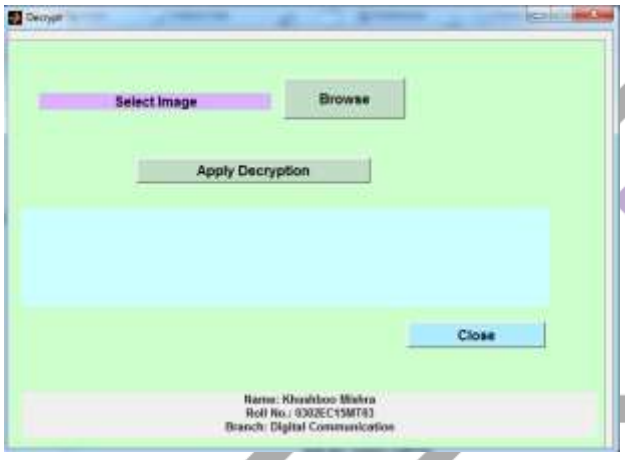

Fig: Image Decryption Basic layout using MatLab

Conclusion

In the proposed system, steganographic method uses the special domain technique that is the LSB Steganography technique which uses the formats like bmp, jpg etc. In this thesis compare PSNR values of the proposed method with with different key values for cover-image *Lena* and message size of 1.09 K.B. This thesis can be extended to a level such that it can be used for different types of image formats like jpeg, bmp etc. in the future. For that we can use the transform domain technique like DWT & DCT.

References

[1] Swathi, A. and Jilani, D. S. (2012). Video Steganography by LSB Substitution Using Different Polynomial Equations. International Journal of Computational Engineering Research, ISSN 2250-3005, Vol. 2, Issue 5, pp. 1620-1623.

[2] Tan, K. T.; Ghanbari, M. and Pearson, D. E. (1998). An objective measurement tool for MPEG video quality. Signal Processing, Elsevier, Vol. 70, No. 3, pp. 279- 294.

[3] Tomar, G. (2012). Effect of Noise on image steganography based on LSB insertion and RSA encryption. IOSR Journal of Engineering, Vol. 2, No. 3, pp. 473-477.

[4] Tseng, H. W. and Chang, C. C. (2004). High capacity data hiding in JPEG compressed images. Institute of Mathematics and Informatics, Vilnius, INFORMATICA, Vol. 15, No. 1, pp. 127–142.

[5] Tyagi, V.; Kumar, A.; Patel, R.; Tyagi, S. and Gangwar, S. S. (2012). Image Steganography using Least Significant Bit with Cryptography. Journal of global research in computer science, Vol. 3, No. 3, pp. 53-55.

[6] Upham, D. (1997). Jpeg–Jsteg, http://www.tiac.net/users/korejwa/jsteg.htm

[7] Vassaux, B.; Nguyen, P.; Baudry, S.; Bas, P. and Chassery, J. M. (2002). Scrambling technique for video object watermarking resisting to MPEG-4. In Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom (pp. 239-244). IEEE.

[8] Venkatraman, S.; Abraham, A. and Paprzycki, M. (2004). Significance of Steganography on Data Security. In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on (Vol. 2, pp. 347-351). IEEE.

[9] Wang, H. and Wang, S. (2004). Cyber warfare: Steganography vs. Steganalysis. Communications of the ACM, Vol. 47, No.10, pp. 76-82.

[10] Wang, X.; Yao, Z. and Li, C. T. (2005). A palette-based image steganographic method using colour quantisation. In Image Processing, 2005. ICIP 2005. IEEE International Conference on (Vol. 2, pp. 1090-1093). IEEE.

[11] Wang, Z.; Bovik, A. C. and Lu, L. (2002a). Why is image quality assessment so difficult?. In Acoustics, Speech, and Signal Processing (ICASSP), 2002 IEEE International Conference on (Vol. 4, pp. 3313-3316). IEEE.

[12] Wang, Z.; Sheikh, H. R. and Bovik, A. C. (2002b) No-reference perceptual quality assessment of JPEG compressed images. In Image Processing. 2002. Proceedings. 2002 International Conference on (Vol. 1). IEEE.

[13] Watson, A. B. (1994a). Image compression using the discrete cosine transform. Mathematica Journal, Vol. 4, No. 1, pp. 81-88.

[14] Watson, A. B. (1994b). Perceptual optimization of DCT color quantization matrices. In Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference (Vol. 1, pp. 100-104). IEEE.

[15] Wayner, P. (2009). Disappearing cryptography: information hiding: steganography and watermarking. Morgan Kaufmann.

[16] Weng, S.; Zhao, Y.; Ni, R. and Pan, J. S. (2009). Lossless data hiding based on prediction-error adjustment. Science in China Series F: Information Sciences, Springer Vol. 52, No. 2, pp. 269-275.

[17] Westfeld, A. and Pfitzmann, A. (2000). Attacks on steganographic systems. In Information Hiding (pp. 61-76). Springer Berlin Heidelberg.

[18] Wu, D. C. and Tsai, W. H. (2003). A Steganographic method for images by pixel value differencing. Pattern Recognition Letters, Elsevier, Vol. 24, No. 9, pp. 1613-1626.

[19] Wu, H. R. and Rao, K. R. (Eds.). (2005). Digital video image quality and perceptual coding. CRC press.

[20] Wu, M. Y.; Ho, Y. K. and Lee, J. H. (2004). An iterative method of palette-based image Steganography. Pattern Recognition Letters, Elsevier, Vol. 25, No. 3, pp. 301-309.

[21] Wu, N. I. and Hwang, M. S. (2007). Data Hiding: Current Status and Key Issues. International Journal of Network Security, Vol. 4, No. 1, pp.1-9.

[22] Yu, Y. H.; Chang, C. C. and Lin, I. C. (2007). A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding, Vol. 107, No. 3, pp. 183-194.
[23] Zhang, T.; Zhang, Y.; Ping, X. and Song, M. (2006). Detection of LSB Steganography based on Image Smoothness. In Multimedia and Expo, 2006 IEEE International Conference on (pp. 1377-1380). IEEE.
[24] Zhang, W.; Zhang, X. and Wang, S. (2007). A double layered ―plus-minus one‖ data embedding scheme. Signal Processing Letters, IEEE, Vol. 14, No. 11, pp. 848-851.