Reliable Detection of LSB Steganography in Greyscale and Color Images

Nitika Mittal
Computer Science, IMS Engineering College, Ghaziabad, India.

Khushboo Khanna
Computer Science, Director at NITD Pvt. Ltd, India.

Abstract – Steganography is that the technique for activity secret data in different information likes still, transmission pictures, text, and audio. Whereas Steganography is that the reverse technique during which detection of the key data is finished within the stego image. Steganography may be classified on the idea of the techniques used classified applied math techniques, pattern classification techniques and visual detection techniques.

In this research, an intensive review report is bestowed chronologically on the BlindImage Steganography for the still stego pictures mistreatment the classification techniques.

Index Terms – Steganography, Information, Pattern Classification.

1. INTRODUCTION

Steganography is a technique of hiding information in digital media. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. One method of providing more security to data is information hiding. The approach to secured communication is cryptography, which deals with the data encryption at the sender side and data decryption at the receiver side. The main difference between Steganography and cryptography is the suspicion factor.

2. RELATED WORK

Stenography Technique

The various Steganography techniques are:

Substitution technique: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc.

Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc.

Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely.

Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero.

Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message. The main aspect of Steganography is to achieve high capacity, security and robustness.

3. PORPOSED MODELLING

We design modules namely stenography and the proposed algorithm is an improved version of LSB based image steganography. In this method, we modify the data image and then XORing the data image pixel with the cover image pixel. The obtained results show that the proposed algorithm provides an improved value of PSNR than LSB based image steganography method. This technique could be combined with other method to improve steganography.

Distortion occurred in different steganos is required by varying the depth of hiding for embedding information in cover image. The relation between depth of hiding used and distortion occurred in the stego images is shown in Fig. that depth of hiding within some LSB region is most suitable for message embedding as the distortion is very small in this region. As the depth of hiding increases beyond preferable region, the distortion becomes noticeable and unsuitable for message hiding.

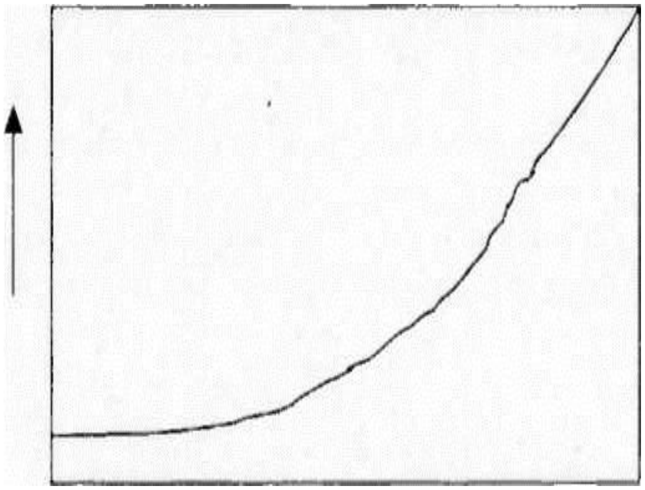


Figure1: Depth Vs Distortion Analysis →

Image compression offers a solution to large image files. Two kinds of image compression are:

- lossless compression
- lossy compression

Both methods save storage space but have differing effects on any uncompressed hidden data in the image.

Lossy compression:

As typified by JPEG (Joint Photographic Experts Group) format files, offers high compression, but may not maintain the original image's integrity. This can impact negatively on any hidden data in the image. This is due to the lossy compression algorithm, which may "lose" unnecessary image data, providing a close approximation to high-quality digital images, but not an exact duplicate. Hence, the term" Loss compression" is frequently used on true-color images, as it offers high compression rates.

Lossless compression:

It maintains the original image data exactly; hence it is preferred when the original information must remain intact. It is thus more favored by steganographic techniques. Unfortunately, lossless compression does not offer such high compression rates as loss compression. Typical examples of lossless compression formats are CompuServe's GIF (Graphics Interchange Format) and Microsoft's BMP (Bitmap) format.

4. RESULTS AND DISCUSSIONS

To hide a message, open a picture file, then enter a parole or choose a key file. The key file are often any file, another picture as an example. This parole or key are treated as a stream of bytes specifying the area between 2 modified pixels. I do not suggest text files, as a result of they will end in a quite regular noise pattern. The longer your key file or parole is, the less regular the noise can seem.

Next step, enter the key message or opt for a file, and click on the Hide button. The appliance writes the length of the message in bytes into the primary picture element. Afterward it reads a computer memory unit from the message, reads another computer memory unit from the key, and calculates the coordinates of the picture element to use for the message-byte. It increments or resets the color element index, to modify between the R, G and B element. Then it replaces the R, G or B element of the picture element (according to the color element index) with the message-byte, and repeats the procedure with consequent computer memory unit of the message. At last, the new picture is displayed. Save the picture by clicking the Save button. If the grayscale flag is ready, all elements of the colorare modified. Grayscale noise is a smaller amount visible in most pictures.

The software requirements for developing the project are as follows:

Framework: Microsoft Visual Studio 2010

- Front End Tool: Windows Application
- Language: C#

In this section of thesis we will discuss about the different modules of the project along with their respective explanations. All the executing steps are depicted with their respective screenshots followed by discussion.

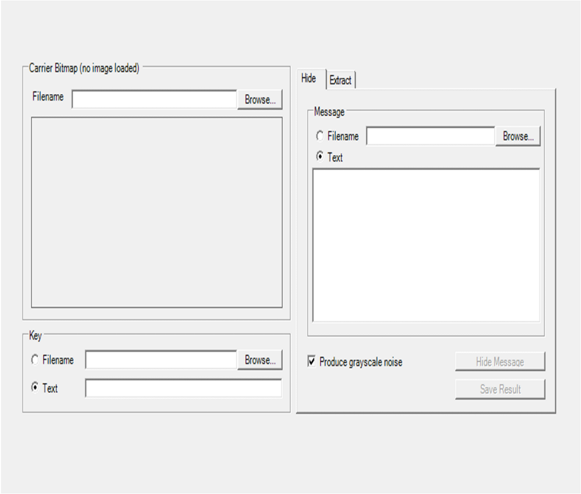
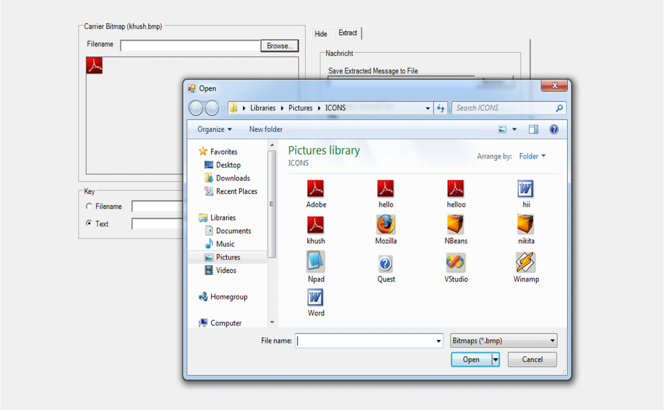
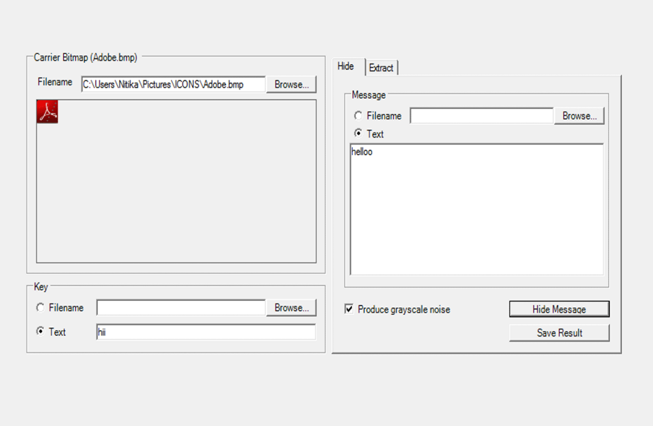


FIG: Front page of designed Steganography

This is the front look of the designed steganography of color image and gray scale image. In this technique we can hide the information in other digital medium to make secret communication. Here user can hide the data in any image or text file using the key.



This is browse the new bitmap image which have to transfer the sender. Behind this sender can hide any image file and any text file using any key. Senders have to use the same size of hidden file as the bit map image, which use to transfer to sender.



Filename: C:\Users\Nitika\Pictures\ICONS\Adobe.bmp

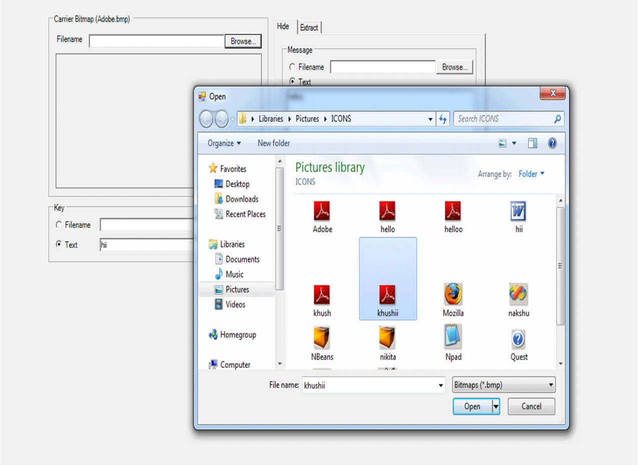
Message: ○ Filename ● Text

helloo

Key: ○ Filename ● Text hii

☑ Produce grayscale noise

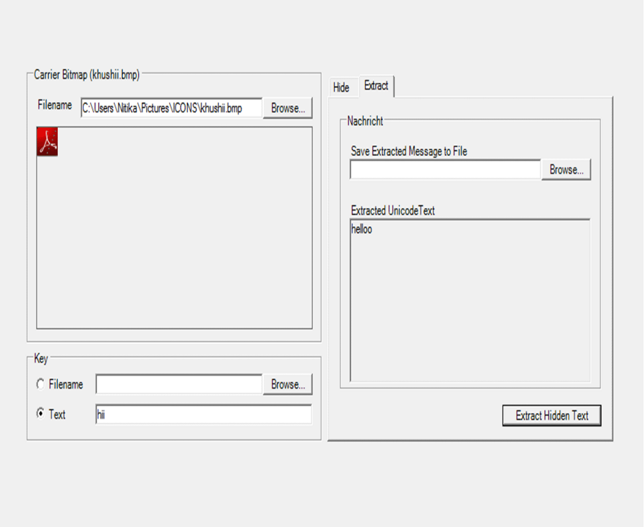
After browse the image, user can hide the data which have to send to sender secretly using key. The key can be of any text file or any image file. After that “Save Result” in bitmap extension.



File name: khushii

At the receiver side extract the image which is send by sender. And the use the same key that has been used by sender to send the data secretly to receiver. After that press the extract key and extract the same data which is hide by sender.

In this section of thesis, we represent the result analysis of the data-hiding algorithms is the stego-signal quality which has been completely demonstrated in previous chapter.



Filename: C:\Users\Nitika\Pictures\ICONS\khushii.bmp

Extracted UnicodeText: helloo

Key: ○ Filename ● Text hii

5. CONCLUSION

The major problem in data-hiding algorithms is the stego-signal quality, which is inversely proportional with hiding capacity. The LSB hiding technique is one of the most simple and famous hiding techniques. However, it suffers from several problems, such as low capacity and security. Several techniques are suggested based on the LSB technique to enhance the quality of the stego-image and sometimes increase the capacity. However, the capacity of most of these methods doesn’t exceed 4 bpp, which is not enough to hide one image in another with the same dimensions.

Also, in LSB-based techniques, if the adversary knows the existence of hidden data, he can extract it easily, while in the proposed method the attacker must have a copy of the cover image to extract the hidden data, but that is impossible because the cover image is unknown.

Future work can think about doing the subsequent modifications to the planned method:

1. Work the planned methodology on color pictures.

2. Modifying the planned approach to plant image within another image.

3. Preserve the key message albeit we have a tendency to do some transformations on the image like rotation, scaling compression.

4. Relate the encoding method with steganography within which we write the message before embedding it within the image so as to extend the protection of the planned method.

REFERENCES

[1] A blind image Steganography based on features from three domains Yuan Liu; Li Huang;Ping Wang; GuodongWang;Control and Decision Conference, 2008. CCDC 2008, Chinese ,2-4 July 2008 Page(s):2933 – 2936.

[2] JPEG Steganography using color correlation and training on clean images only Hong Cai;Agaian,S.S.;Machine Learning and Cybernetics, 2008 International Conference on Volume 7, 12 -15 July 2008 Page(s):3710 – 3713.

[3] A New Steganography Method Using High-pass Filter for JPEG Image Han-ling Zhang;Shu-yi Wang; Electronic Commerce and Security,2008 International Symposium on 3-5 Aug. 2008 Page(s):165 – 168.

[4] Steganography Based on Co-occurrence Matrix of Differential Image Ziwen Sun; Maomao Hui; Chao Guan;Intelligent Information Hiding and Multimedia Signal Processing, 2008,IIHMSP '08 International Conference on 15-17 Aug. 2008 Page(s):1097 – 1100.

[5] Steganography of LSB Matching Based on Co-occurrence Matrix and Removing Most Significant Bit Planes Abolghasemi, M.;Aghainia,H.; Faez, K.; Mehrabi, M.A.;Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on 15-17 Aug. 2008 Page(s):1527 – 1530.

[6] Image universal Steganography based on wavelet packet transform Xiangyang Luo; Fenlin Liu; Jianming Chen; Yining Zhang; Multimedia Signal Processing, 2008 IEEE 10th Workshop on Digital 2008 , Page(s): 780 - 784 .

[7] Features-Pooling Blind JPEG Image SteganographyChiew Kang Leng; Pieprzyk, J.;Computing: Techniques and Applications, 2008. DICTA '08.Digital Image1-3 Dec. 2008 Page(s):96-103.

[8] Blind image Steganography based on run-length histogram analysis Jing Dong; TieniuTan;Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on Digital Object Identifier: 10.1109/ICIP.2008.4712192 Publication Year: 2008 , Page(s): 2064 – 2067 .

[9] Detection of BPCS-Steganography using SMWCF Steganography and SVM Lopez- Hernandez, Julio; Martinez-Noriega, Raul; Nakano-Miyatake, Mariko; Yamaguchi, Kazuhiko;Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on 7-10 Dec. 2008 Page(s):1 - 5 .

[10] Steganography of LSB matching based on histogram features in grayscale image Xu Mankun; Li Tianyun; Ping Xijian;Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on 10- 12 Nov. 2008 Page(s):669 – 672.

[11] A New Blind Steganography Method for JPEG Images Xiang Li; JianhuaLi;Computer Science and Software Engineering, 2008 International Conference on Volume 3,12-14 Dec. 2008 Page(s):939-942 .

[12] Multi-class Steganography for Jpeg stego algorithms Ping Wang; Fenlin Liu; Guodong Wang; Yifeng Sun; DaofuGong;Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on 12- 15 Oct. 2008 Page(s):2076 - 2079 .

[13] Universal JPEG Steganography based on microscopic and macroscopic calibration Fangjun Huang; Jiwu Huang; Bin Li;Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on 12- 15 Oct. 2008 Page(s):2068 - 2071 .

[14] Detect Information-Hiding Type and Length in JPEG Images by Using Neuro-fuzzy Inference Systems Liu, Qingzhong; Sung, Andrew H.; Image and Signal Processing,2008. CISP '08. Congress on Volume: 5 ,2008 , Page(s): 692 - 696 .

[15] Steganography of multi-class JPEG images based on expanded Markov features and polynomial fitting Qingzhong Liu; Sung, A.H.; Ribeiro, B.M.; Ferreira, R.; Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence).IEEE International Joint Conference ,2008 , page(s): 3352 - 3357 . [13] Universal Steganography Using Color Correlation and Feature Fusion Yuan-luTu; Sheng- rong Gong; Information Science and Engineering, 2008. ISISE '08. International Symposium on Volume: 1, Publication Year: 2008 , Page(s): 107 - 111 .

[16] An Investigation of Genetic Algorithm on Steganography Techniques Xiao Yi Yu; Aiming Wang; Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. Fifth International Conference ,2009 , Page(s): 1118 - 1121 .

[17] Feature-Based Steganography for JPEG Images Zhuo Li; Kuijun Lu; Xianting Zeng; Xuezeng Pan; 2009, Page(s): 76 - 80 .

[18] Universal Image Steganography Based on Wavelet Packet Decomposition and Empirical Transition Matrix in Wavelet Domain Xiaoyuan Yang; Yu Lei; Xiaozhong Pan; Jia Liu; Computer Science-Technology and Applications, 2009. IFCSTA '09. International Forum on Volume: 2 ,2009 , Page(s): 179 – 182.

[19] Intelligent detection of LSB stego anomalies in images using soft computing paradigms Geetha, S.; Sindhu, S.S.; Ishwarya, N.; Mohan, A.; Amuthayazhini, P.; Kamaraj, N.; Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on Publication Year: 2009 , Page(s): 1 - 5 .

[20] An Image Steganography Method Based on Characteristic Function Moments of Wavelet SubbandsZiwen Sun; Hui Li; Zhijian Wu; Zhiping Zhou; Artificial Intelligence and Computational Intelligence, 2009. AICI '09. International Conference on Volume: 1 , 2009, Page(s): 291 - 295 .