ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 405-408

Extracting Spread-Spectrum Hidden Data from Picture Representation

[1] R NEELIMA DEVI , [2] B.RANJITH

[1] M.Tech Research Scholar, Priyadarshini Institute of Technology and Science for Women
[2] HOD-CSE, Priyadarshini Institute of Technology and Science for Women

Abstract: In this paper, we introduce a novel high bit rate LSB Picture information concealing system. The fundamental thought of the proposed LSB computation is information installing that causes negligible implanting contortion of the host picture. Utilizing the proposed two-stage result, information concealing bits are inserted into higher LSB layers, resulting in expanded vigor against clamor expansion or picture layering. Listening tests demonstrated that the perceptual nature of information hided picture is higher on account of the proposed technique than in the standard LSB strategy.

Index Terms: Higher LSB, Guard Pixels, Stegnography,Multi- carrier, Information hiding, Data Encryption.

I INTRODUCTION

Data tracking and tampering are rapidly increasing in everywhere like online tracking, mobile tracking etc. So we need a secured communication scheme for transmitting the data. For that, we are having many data hiding schemes and extraction schemes. Data hiding schemes are initially used in military communication systems like encrypted message, for finding the sender and receiver or it's very existence. Initially the data hiding schemes are used for the copy write purpose. In [1] Fragile watermarks are used for the authentication purpose, i.e. to find whether the data has been altered or not. Likewise the data extraction schemes also provide a good recovery of hidden data .This is the goal of the secured communication.

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Image file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or image which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it. There are many to embed information into a popular media using steganography. A good example of this is the relationship between are coded song, and its lyrics. The image file containing the recording is much larger than the song lyrics stored as a plain ASCII files.

In this Paper we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. The LSB method used for this project which satisfies the requirement of steganography protocols. This research will include implementation of steganographic algorithm for

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 405-408

encoding data inside video files, as well as technique to dynamically extract that data as original.

II RELATEDWORK

There are many data hiding and data extraction schemes are comes into existence. The important data hiding technique is steganography. It is differ from cryptography in the way of data hiding. The goal of steganography is to hide the data from a third party whereas the goal of cryptography is to make data unreadable by a third party. In [2] the steganalysis method is used. The goal of steganalysis is to determine if an image or other carrier contains an embed message. In my project the concept of Watermarked Content only attack" in the watermarking security context is taken.i.e the blindly recovery of data is considered. In [3],in steganalysis concept it is said to be Universal Steganalysis means instead of using any priori information ,they take into account all available steganography methods to devise a single steganalysis framework. This approach can detect any steganography if sufficient numbers of cover and stego images have been taken into account during the design process. In [4] spread spectrum embedding algorithm for blind steganography have based on the understanding that the host signal acts as a source of interference to the secret message of interest. Such knowledge can be useful for the blind receiver at the recovery side to minimize the recovery error rate for a given host signal. To increase the security and payload rate the embedded will take multicarrier embedding concept. In [5] the spread spectrum communication is explained. Here a narrow band signal is transmitted over a much larger bandwidth such that the signal energy present in any single frequency is imperceptible. Similarly in SS embedding scheme, the hidden data is spread over many samples of host signal by adding a low energy Gaussian noise sequence. The DCT transformation is taken for embedding purpose as a carrier since it is a fast algorithm and for it's efficient implementation. In [6] the Generalized Gaussian Distribution (GGD) has been used to model the statistical behavior of the DCT coefficients. In [7] there are many extraction procedures to seek the hidden data. Built is having some disadvantages. Iterative Least Square Estimation (ILSE) is prohibitively complex even for moderate values. Pseudo-ILS (ILSP) algorithm is not guaranteed to converge in general and also it provides measurably worse results. So, these two algorithms coupled and so called Decoupled weighted ILSP (DW-ILSP).But here also have a disadvantage like, it may not be valid for large N.

III. PROPOSED METHODOLOGY

3.1. Algorithms

Data Hiding:-

1. Select an Image
2. Split an Image into multi-carrier objects.
3. Select a multi-carrier image.
4. Select Secrete data for hiding.
5. Encrypt data with shifting method
6. Split data into equal number of carrier objects.
7. Apply Higher LSB Method for replacing pixels bits with encrypted data bits by taking one multicarrier image object & secret data segment.
8. Repeat Step 3 & Step 7 until all encrypted data segments not hidden into multi carrier images.
9. Join multi carrier's objects to create single image.
10. Stop

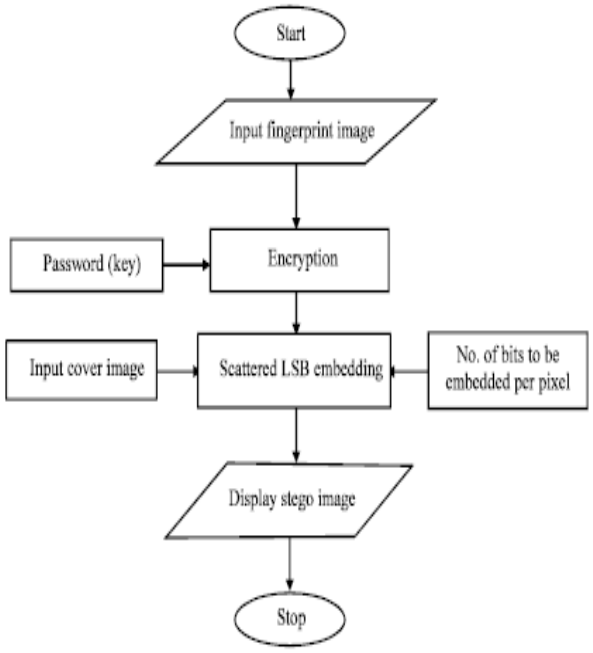

Fig 1: Data Hiding in an Image

Data Extraction:-

1. Select a Stego Image.
2. Split stego Image.
3. Apply Higher LSB Extraction algorithm.
4. Select length Key.
5. Extract data bits from 1 to 5 LSB color pixels

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 405-408

bits.
6. Generate Data.
7. Decrypt Data.
8. Stop

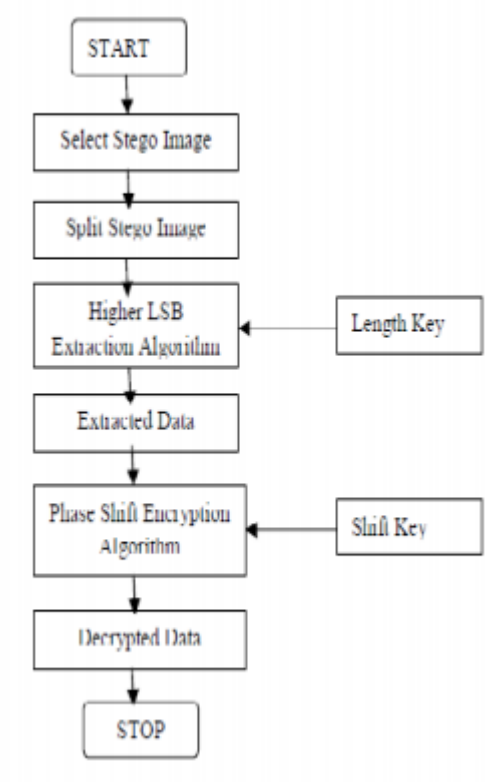

Fig 2. Data Extraction

IV EVALUTION

The proposed method is to extract the hidden data from the digital media. Here blindly recovery of data is considered. That is the original host end embedding carrier is not need to be known. This method uses multicarrier embedding and DCT [15] transformation for the embedding the data into the host image. The M-IGLS algorithm is used for the extraction purpose. This algorithm is a low complexity algorithm and it attains the probability of error recovery equals to known host and embedding carriers. It is used as a tool to analyze the performance of the data hiding schemes.

Fig.3 Extracted Data

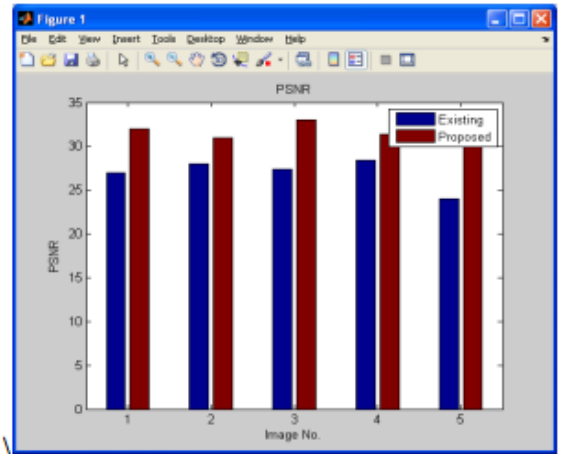

Fig. 4 Graph for PSNR verses image number

V CONCLUSION

We presented a reduced distortion algorithm for LSB image steganography. The key idea of the algorithm is data hiding bit embedding that causes minimal embedding distortion of the host image. Visualization tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 1th to 5LSBlayer without affecting the perceptual transparency of the data hided image signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant cryptography provided for data security.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," Proc. IEEE (Special

Issue on Identification and Protection of Multimedia Information), vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information), vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," IEEE Signal Processing Magazine, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in Information Hiding, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," Communications of the ACM, vol. 47, pp. 76-82, Oct. 2004.

[7] C. Cachin, "An information-theoretic model for steganography," in Proc. 2nd Intern. Workshop on Information Hiding, Portland, OR, Apr. 1998, pp. 306-318.

[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in Advances in Cryptology: Proc. CRYPTO'83. New York, NY: Plenum, 1984, pp. 51-67.

[9] J. Fridrich, Steganography in Digital Media, Principles, Algorithms, and Applications. Combridge, UK: Combridge Univeristy Press, 2010.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," IEEE Trans. Inform. Theory, vol. 54, pp. 2706-2722, June 2008.

[11] Federal plan for cyber security and information assurance research and development, Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.

[12] R. Chandramouli, "A mathematical framework for active steganalysis," ACM Multimedia Systems Special Issue on Multimedia Watermarking, vol. 9, pp. 303-311, Sept. 2003.

[13] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Proc., vol. 51, pp. 898-905, Apr. 2003.

[14] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Proc., vol. 6, pp. 1673-1687, Dec. 1997.

[15] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain water- marking techniques for still images: Detector performance analysis and a new structure," IEEE Trans. Image Proc., vol. 9, pp. 55-68, Jan. 2000.

[16] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, pp. 273-284, Sept. 2001.

[17] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of wa- termarking algorithms for improved resistance to compression," IEEE Trans. Image Proc., vol. 13, pp. 126-144, Feb. 2004.

[18] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in Proc. IEEE Intern. Conf. Image Proce. (ICIP), Singapore, Oct. 2004, pp. 1561-1564.

[19] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley, "Blind iterative recovery of spread-spectrum steganographic messages," in Proc. IEEE Intern. Conf. Image Proc. (ICIP), Genova, Italy, Sept. 2005, vol. 2, pp. 11-14.

[20] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," IEEE Trans. Image Proc., vol. 16, pp. 391-405, Feb. 2007.