ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Fuzzy based selection of wavelets for Image Steganography

Manika Bhatt

M.Tech, Computer Science & Engg., Shree Siddhivinayak Group of Institutions, Yamuna Nagar, India

Abstract: In this paper, we have proposed a new image steganography scheme which is a Fuzzy based selection of wavelets. There are some attack forms to data and informations i.e. hacker, trojan horse attack, cracker and others. In consequence, today various efforts have been conducted to take care of data security and overcome attacks is previously already there is a way to take care of data security that is recognized by the name of cryptography. With cryptography for secret data it security is maintained nevertheless from cipher text that randomized will be easily detected and awake third party about secretness of files. For that deep steganography is applied which in Greek words means "message are hidden" (covered writing) in effort to take care of secretness of datas. Steganography is the way to hide the data. In the current paper we are going to present different aspects of steganography from different authors.

Keywords: Steganography, Cryptography, Encryption, Fuzzy, Matlab.

1. INTRODUCTION

Steganography is the Science and art of communicating in a way which hides the existence of the communications. Important information is firstly hidden in a hosts data such as digital images, audio,or vedio,text etc and then transmitted secretly to the receiver.

The main aim in steganography is to hide the very existence of the messages in the cover medium. Cryptography and Steganography are counter parts in digital security.

The obvious advantage of steganography over cryptography is that messages do n't attracts attention to themselves, to messengers or to recipients. Also in the last decade has been seen an exponential growth in the use of multimedia data over the Internet.

These include Digital Image, Audio and Video files. In this rising of digital content on the internet has further accelerated the research effort devoted to steganography.

1.1 Types Of Steganography:

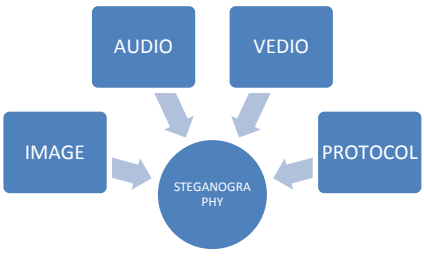

Figure 1. Steganography Types

2. STEGANOGRAPHY SYSTEM

It is assumed that the sender wishes to sends via Steganographic transmission messages to a receiver. The sender starts with a cover message which is an input to the stegosystem in which the embedded message will be hidden. The hidden messages are called the embedded messages. A Steganographic algorithm combined the cover messages with the embedded messages which is something to be hidden in the cover .The algorithm may or may n't use a Steganographic keys (stego key) which is additional secret data that may be needed in the hidden process. The same keys (related one) are usually needed to extract the embedded message again. The output of the Steganographic algorithms are the stego messages.The cover massages and stego messages must be of the same data types but the embedded message may be of another data type. The receiver reverses the embedding process to extracts the embedded messages.

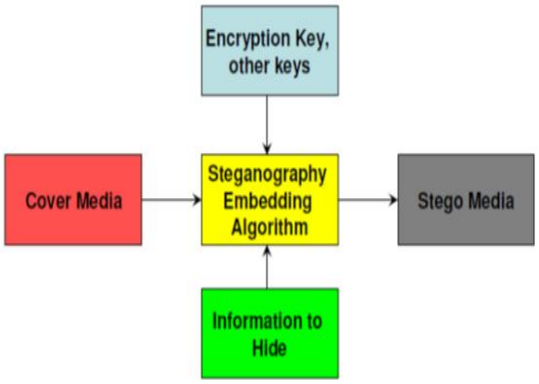

Figure 2. Basic Steganographic Process

3. EMBEDDING DATA

The goal of steganography is to conceal data. There are a few features and restrictions to successfully hide data. "The goal is for the data to remain "hidden."

The word "hidden" has two meanings here (a) the data can be "hidden" and not visible to the human eye (b) the data can be visible and still not visible to the human eye. If the focus is deterred from the data, the data will not be seen, which means that it is "hidden".

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

The following guidelines represent a few features and restrictions when embedding data.

- Often although it is not necessary the hidden messages will be encrypted. This meets a requirement posed by the "Kerckhoff principle" in cryptography. This principle states that the security of the system has to be based on the assumption that the enemy has full knowledge of the design and implementation details of the steganographic system.
  The only missing information for the enemy is a short, easily exchangeable random number sequence, the secret key. Without this secret key, the enemy should not have the chance to even suspect that on an observed communication channel, hidden communication is taking place.
  Most of the software that we will discuss later meets this principle. When embedding data Bender et al. reminds us that it is important to remember the following restrictions and features:
- The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible. This does n't mean the embedded data needs to be in-visible it is possible for the data to be hidden while it remains in plain sight.
- The embedded data should be directly encoded into the media rather than into a wrapper or header to maintain data consistency across formats.
- The embedded data should be as immune as possible to modifications from intelligent attack or anticipated manipulations such as filtering and re-sampling.
- Some degradations or distortions of the embedded data can be expected when the cover data is modifing. To minimize this error correcting codes should be used.
- The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can still be extracted when only portion of the cover data are available.
  For example, if only be a part of images are available the embedded data should still be recoverable.

4. LITERATURE REVIEWS

Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place.

4.1 LSB Substitution Method :

Kekre et al. proposed the least significant bit (4LSB) substitution method that has been used earlier. 4LSB method was implemented for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media.

"The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present."

By using this proposed algorithm, we can hide our file of any format in an image and audio file. We can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it. LSB gives high level of embedding but at the cost of image quality.

If more bits are stuffed to hide the data then the secret image traces are visible on the cover images.

4.2 Color Image Steganography based on Module Substitutions:

An effective color image steganography method based on the module substitutions was proposed. Here in accordance with the base-value of the blocks, a variety of secret bits is embedded to a RGB trichromatic.

System by three types of module substitutions, more specifically, to alleviate further color distortion and obtain a larger hidden capacity, the R-, G- and B-component is encoded by Mod u, Mod u-v, and Mod u-v-w substitution, respectively.

Experiments show that both PSNR and hiding rate generated by the proposed method are better than those generated by the above reported scheme. In addition, the resulting perceptual quality is good.

4.3 An Adaptive Image Steganography Based on Depth-varying Embedding:

Steganography technique is a means of covert communication. This technique is an adaptive image steganography with high capacity and good security. Based on local complexity of a cover image, varying-depth embedding is used to improve the imperceptibility and decrease distortions in it.

Experimental results show that this steganography technique may provide higher capacity and better resistance to several well-known steganalytic methods.

4.4 Steganography Using JPEG-Compressed Images:

In 1999, Kobayashi et al. gave a novel steganography method based on JPEG. Here we take advantage of the quantization error resulting from processing the JPEG-compressed image with two different scaling factors.

One of the scaling factors is used to control the bit rate of the stego-image while the other is used to guarantee the quality of the stego-image.

Our experimental results shows that the proposed steganography method can provide a high information hiding capacity and successfully control the compression ratio and distortion of the stego- image.

4.5 A New Image Steganography Based on 2k Correction and Edge-Detection:

It is a new image steganography scheme proposed by Lie-Chang, which is a kind of spatial domain technique. In order to hide secret data in cover-image, we use the just noticeable difference (JND) technique and method of contrast sensitivity function (CSF).

This is an edge-detection which uses part information of each pixel-value. In order to have better imperceptibility, mathematical method which is the 2k correction is proposed and shows better imperceptibility.

To prove this scheme, several experiments were performed, and compared the experimental results with the related previous works.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

5.COMPARISON OF DIFFERENT STEGANOGRAPHY TECHNIQUES

LSB substitution Method	**Color Image Based on Module substitution**	**Adaptive image steganography Based on DVE**	**Steganography Using JPEG-Compressed Images**	**Steganography Based on 2k Correction and Edge-Detection**
Uses Simple approach to embed.	Perceptual Quality is good.	Resistant to common steganalytic methods.	Steganography can take place between the two stages: lossy and lossless.	Edge detection uses part information of each pixel value. For better imperceptibility 2k correction method is used.
Do not degrade the image to the point of being noticeable.	PSNR and hiding rate are better than LSB.	High capacity and good security.	The data can be hidden in the redundant bit of the image object.	It can embed more data and shows better intercept ability.
Extremely vulnerable to attacks & more stuffed bits lead to secret image traces on cover.	Bits are embedded to RGB trichromatic system by 3 type of module substitution.	Difficult to detect artifacts in form of pair of values.	The hidden message could be damaged.	To hide secret data in cover-image, we use just noticeable difference (JND) technique and (CSF) method

6. CONCLUSION

Steganography is the arts of covered or hidden writing. The purpose of steganography is covert communication to hide the existence of messages from third party. In this paper provides a ongoing researhs in context for steganography the emphasis is on digital applications focusing on hiding information in online images. For future we will do the stegnography in transform domain.

7. REFERENCES

[1] Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, ?Spread Spectrum Image Steganography?, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999.

[2] Jessica Fridrich, Miroslav Goljan, Binghamton, Department of Electrical Engineering, Binghamton, NY,? Practical Steganalysis of Digital Images ? State of the Art?, Conference , San Jose CA , ETATS-UNIS (21/01/2002)

[3] Kevin Curran, Internet Technologies Research Group, University of Ulster, Karen Bailey, Institute of Technology, Letterkenny, Ireland,? An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2

[4] Sabu M Thampi, Assistant Professor, Department of Computer Science & Engineering, LBS College of Engineering, Kasaragod,Kerala- 671542, S. India ,? Information Hiding Techniques: A Tutorial Review?, ISTE-STTP on Network Security & Cryptography, LBSCE 2004

[5] Kefa Rabah, Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey,? Steganography-The Art of Hiding Data?, Information Technology Journal 3 (3): 245-269, 2004,ISSN 1682-6027

[6] Der-Chyuan Lou and Chia-Hung Sung,? A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem?, IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 6, NO. 3, JUNE 2004

[7] Hsien-Wen Tseng and Chin-Chen Chang, Department of Computer Science and Information Engineering National Chung Cheng University, Chaiyi, Taiwan,? Steganography Using JPEG-Compressed Images?, Proceedings of the Fourth International Conference on Computer and Information Technology (CIT?2004). Sept. 2004

[8] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang,? Image steganographic scheme based on pixel-value differencing and LSB replacement methods?, IEEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[9] Ching-Yu Yang, Department of Computer Science and Information Engineering, National Penghu University Penghu, Taiwan,? Color Image Steganography based on Module Substitutions?, Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication:?2007 ISBN:0-7695-2994-1

[10] S .K. Moon , R.S. Kawitkar, PICT, Pune and SCOE, Pune, INDIA,? Data Security using Data Hiding?, International Conference on Computational Intelligence and Multimedia Applications 2007.

[11] Nameer N. EL-Emam, Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan,? Hiding a Large Amount of Data with High Security Using Steganography Algorithm?, Journal of Computer Science 3 (4): 223-232, 2007,ISSN 1549-3636 2007 Science Publications