International Journal of Recent Research and Review, Vol. VIII, Issue3, September 2015
ISSN 2277 – 8322

Hiding Data behind Image through Integer Wavelet Transform for Enhance Capacity and Security

Shweta Gupta, Ram Kishan Bairwa
Kautilya Institute of Technology & Engineering, Jaipur, India
Email: ramkishan.bairwa@gmail.com

***Abstract* - Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography, which only conceals the content of the message, not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper, we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval. Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient. Naturally, there are security agents who would like to fight these data hiding systems by steganalysis, i.e. discovering covered messages and rendering them useless. There is currently no steganography system that can resist all steganalysis attacks. In this paper, we propose a novel GA evolutionary process to make a secure steganographic encoding on JPEG images. In the proposed work steganography step is based on genetic algorithm and OPAP that is proved the least vulnerable steganographic system. A combination of LSB approach and Maximum Absolute Difference (MAD) for the image quality are used as the GA fitness function. The model presented here is based on JPEG images; however, the idea can potentially be used in other multimedia steganography as well.**

***Keywords*- Steganography, cryptography, genetic algorithm**

I. INTRODUCTION

What you see is not always, what you get! Thanks to a new technology, steganography, the art of hiding messages inside other messages, is now gaining more popularity and is used on various media such as text, images, sound, and signals. However, none of the existing schemes can yet shield against all detection attacks. Using genetic algorithms that are based on the mechanism of natural genetics and the theory of evolution, we can design a general method to guide the steganography process to the best position for data hiding.

Steganography is the method of hiding digital information within any computer files/ image. Steganography offers an essential alternative to image integrity and authenticity problem. It is a kind of data hiding technique that provides another way of security protection for digital image data. Steganography can be achieved in two ways. One is spatial domain steganography and another is frequency domain steganography. In spatial domain steganography, the hidden information is directly embedded into image pixels. In frequency domain steganography the image pixels are first transformed into frequency domain using discrete Fourier transformation/ discrete cosine transformation / discrete wavelet transformation etc. then the information is embedded on it. In addition to hide, the information Genetic Algorithm is included in the research work to incorporate another layer of security as well as to minimize the difference between the source and

embedded image pixel for more sensitive application like military people, research institute and medical diagnosis etc. The most common method to make this alteration is usage of the least-significant bit (LSB) developed through masking, filtering and transformations on the source image.

Cryptography is a technique for securing the secrecy of communication. Many different encrypt and decrypt methods have been implemented to maintain the secrecy of the message. , it may also be necessary to keep the existence of the message secret. Steganography is the art and science of invisible communication of messages. It is done by hiding information in other information, i.e. hiding the existence of the communicated information. In image steganography, the information is hidden in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high-speed delivery channels. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the message content secret whereas in steganography focus on keeping the existence of a message secret. Steganography and cryptography are the ways for protecting information from unwanted parties. Watermarking and fingerprinting are the other technologies that are closely related to steganography. They are mainly concerned with the protection of intellectual property. In watermarking, all of the instances of an object are “marked”. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. On the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers in fingerprinting. With this the intellectual property of owner to identify customers who break their licensing agreement by supplying the property to third parties. This work reviews the LSB algorithm and DWT algorithm used for image steganography to illustrate the security potential of steganography for business and personal use [1].

II. RELATED WORK

In [2], Chao Hsu *et.al* presented a data-hiding technique namely the bipolar multiple number base to provide capabilities of authentication, integration, and confidentiality for an electronic patient record (EPR) transmitted among hospitals through the Internet. This technique can be used for hiding those EPR related data such as diagnostic reports, electrocardiogram, and digital signatures from doctors or a hospital into a mark image representing the mark of a hospital which is used to identify the source of an EPR. The bipolar multiple bases are a number system use multiple positive and negative base numbers to represent the numbers. The proposed technique uses the tolerant error (TER) between the mark image and its JPEG decompressed image to obtain the base numbers.

In [3], C. C. Thein *et.al* proposed a simple and fast method for high-hiding capacity based on the modulus operation. A good image vision quality can be achieved by using this method without the need for post-processing. Although, this method is almost as simple as the LSB method in both embedding and extracting, it has a high-hiding capacity in which it can hide a 256 × 256 or 256 × 512 image in a 512 × 512 host image.

A novel steganographic method based on least significant-bit (LSB) replacement and pixel-value differencing (PVD) method is developed by Wu *et. al* [4]. The PVD method depends on the difference between two consecutive pixels. A smooth area in an image gives a small difference value but an edged area gives a large difference value. In the smooth areas, LSB method is used to hide the secret data into the cover image while using the PVD method in the edged areas. The proposed method can hide much larger information and maintains a good visual quality of stego-image as compared with the PVD method being used alone.

In [5], Yu, Chang *et.al* presented a prediction based image-hiding scheme that embeds secret data into compression codes during image compression. This scheme employs a two-stage structure: a prediction stage and an entropy coding stage. The secret data is embedded

into the difference values of a given image after the prediction stage is performed. According to the experimental results, the hiding capacity is high and image quality is better than Jpeg–Jsteg.

In [6], Li, Leung *et.al* introduced a new image hiding scheme by exploring the block similarity between the cover-image and the secret-image. Both of the cover image and the secret image are 8- bit gray scale images. Based on the block difference, the best match cover image block of the secret image is selected. Then, the error-matrix, the normalized-error-matrix, the difference-degree and the quantized-error-matrix between the cover-image block and secret-image block are computed. After that, the normalized-error-matrix and quantized error-matrix is used to modify the cover-image block. This scheme provides a high quality and the secret-image is completely extracted.

In[7], EL-Emam introduced a new algorithm based on hiding large data into colour bitmap(BMP) image by using adaptive image segmentation and adaptive image filtering of the cover-image. All pixels in cover-image are segmented into random numbers of uniform or non uniform segments,(non-uniform which is more secure than uniform segments because it used to carry the input data) after that applying a compression scheme on the secret data file to increase the amount of hiding secret data and perform encryption on secret data. In addition, the pixels in the cover image are selected randomly rather than sequentially by using a new concept called ‘main cases and sub cases’ for each byte in one pixel. The algorithm which is described by pseudo-code is presented and it is possible to implement a steganography algorithm to hide a large amount of data into a carrier bitmap image.

In[8], Yu, Chang *et.al* proposed a steganographic method for hiding a colour or a gray scale secret image in a true colour host image. There are three image-hiding types in the scheme: hiding a colour secret image in a true colour image, hiding a palette-based 256-color secret image in a true colour image, and hiding a gray scale image in a true colour image, which depends on the secret image that is to be hidden in a true colour host image. In all three types of hiding, secret data are encrypted by data encryption standard (DES) method before they are embedded into the host image. The hiding capacity and good image quality are the results in that proposed method.

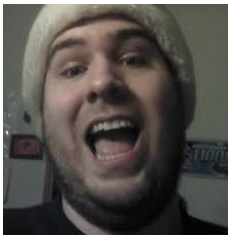
III. PROPOSED WORK

The proposed implementation of hiding text message behind the image in steganography application is depends on used operating system, processor and RAM, so that the operating system should be 32-bit windows OS with 1.84 GHz processor and 2 GB RAM (minimum requirement). The proposed method can applied on 512x512 colored or gray scaled images as shown in Fig. 1.1.

Apple

Child

Fox

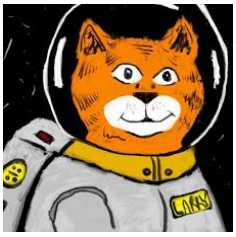


Man

Game

Car

Home



Cartoon

Fig. 1.1 Input Cover Images

The proposed work is done on 2 set of data image as shown in previous section. Both cover images have utilization of 100% and their respective accomplished results of reversible statistical analysis are as follows:

TABLE 1.1
VARIOUS VALUES FOR APPLE

For Jet	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.00043184	0.40555	0.36939
S_m-S_{-m}	0.0015642	0.40347	0.37095

TABLE 1.2
VARIOUS VALUES FOR CHILD

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.37183	0.40555	0.3683
S_m-S_{-m}	0.36987	0.40347	0.36938

TABLE 1.3
VARIOUS VALUES FOR FOX

For Jet	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.36815	0.40555	0.36641
S_m-S_{-m}	0.37077	0.40347	0.36962

TABLE 1.4
VARIOUS VALUES FOR MAN

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.36519	0.40555	0.37408
S_m-S_{-m}	0.37207	0.40347	0.36539

TABLE 1.5
VARIOUS VALUES FOR GAME

For Jet	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.37083	0.40555	0.36846
S_m-S_{-m}	0.37073	0.40347	0.37207

TABLE 1.6
VARIOUS VALUES FOR CAR

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.3649	0.40555	0.36544
S_m-S_{-m}	0.36808	0.40347	0.36593

TABLE 1.7
VARIOUS VALUES FOR HOUSE

For Jet	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.36176	0.40555	0.36546
S_m-S_{-m}	0.37477	0.40347	0.36568

TABLE 1.8
VARIOUS VALUES FOR CARTOON

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.3653	0.40555	0.36447
S_m-S_{-m}	0.36643	0.40347	0.36498

Tables 1.1 to 1.8 have shown the values of $|R_m-R_{-m}|$ and $|S_m-S_{-m}|$ that represent the RS-steganalysis on the regular and singular block. It can be seen that the value of $|R_m-R_{-m}|$ and $|S_m-S_{-m}|$ increases from initial value before embedding and after embedding that exhibits a strong correlation in potential of RS-analysis and the designed module. At initial stage, the values are less, after embedding the message, values increases and finally after applying optimal pixel adjustment process values are decreasing. Human visual system is not able to differentiate the colored images with PSNR more than 36 dB.

TABLE 1.9
COMPARISON OF CAPACITY AND PSNR FOR 4-LSBS

Cover Image	Hiding Capacity (bits)	Data Size (KB)	PSNR (dB)
Apple	2137696 (4-LSBs)	260	26.11
Child	2137696 (4-LSBs)	260	34.80
Fox	2137696 (4-LSBs)	260	67.12
Man	2137696 (4-LSBs)	260	74.14
Game	2137696 (4-LSBs)	260	38.88
Car	2137696 (4-LSBs)	260	15.56
House	2137696 (4-LSBs)	260	46.22
Cartoon	2137696 (4-LSBs)	260	43.61

Fig. 1.2 shows the images after embedding with 4-LSBs. As we compare these embedded images with the input cover images (fig. 1.1), we realize that there are no significant changes in images. The embedded images look like the same as cover images. So the attackers cannot realize in between the communication of two parties that secret message is embedded in these images.

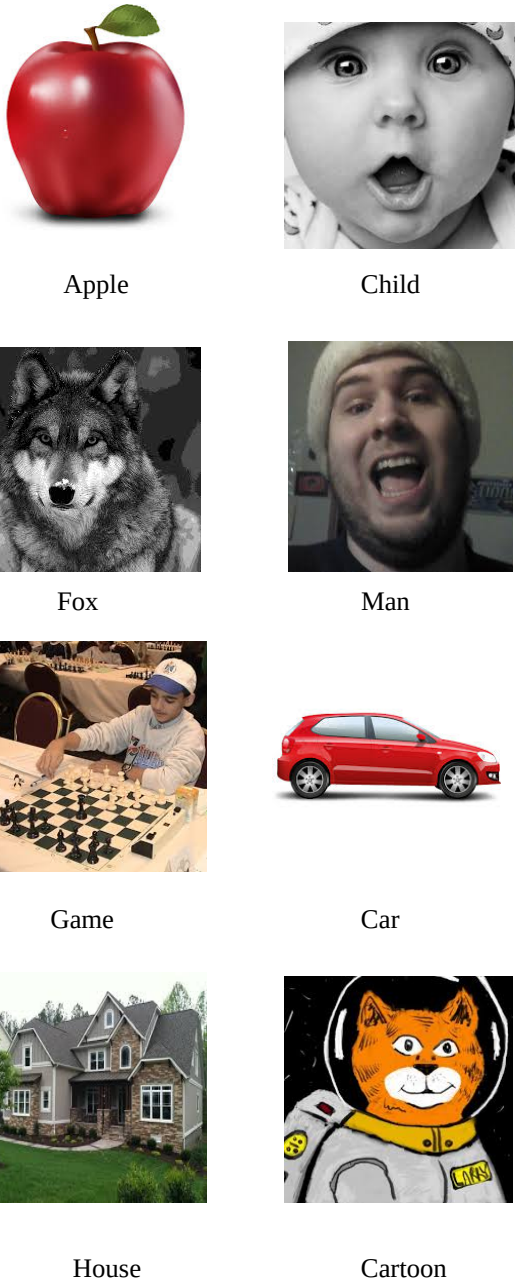
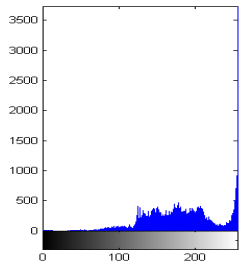
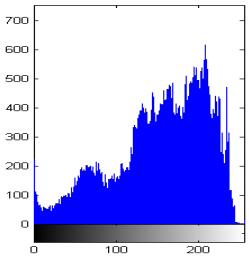


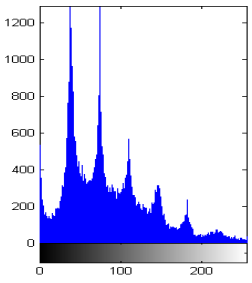
Fig. 1.2 Images after embedding data



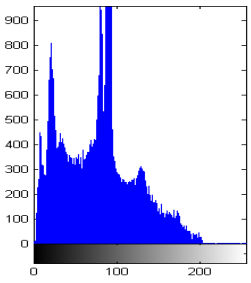
a) Histogram of Apple



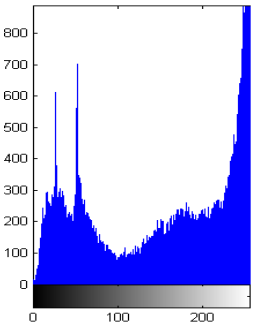
b) Histogram of Child



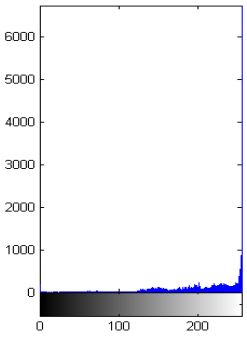
c) Histogram of fox



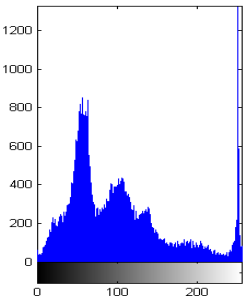
d) Histogram of man



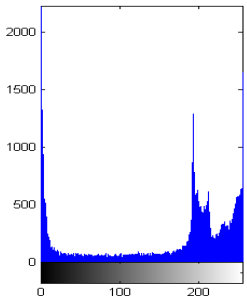
e)Histogram of game



f)Histogram of car



g) Histogram of house



h) Histogram of cartoon

Fig. 1.3. Input cover images histograms

Fig. 1.3 shows the histogram of input cover images. Now the various algorithms such as data embedding, RS analysis and genetic are applied on the cover images. The output stegified image histogram after embedding the data is same as fig. 1.3.

The proposed work considering different image such as gray scale and colored. It can be easily seen by results that proposed research work has better data hiding capacity, 100% utilization, better PSNR value and the best security against attacks as compared with all existing methods. PSNR value comparisons of different images are as shown below:

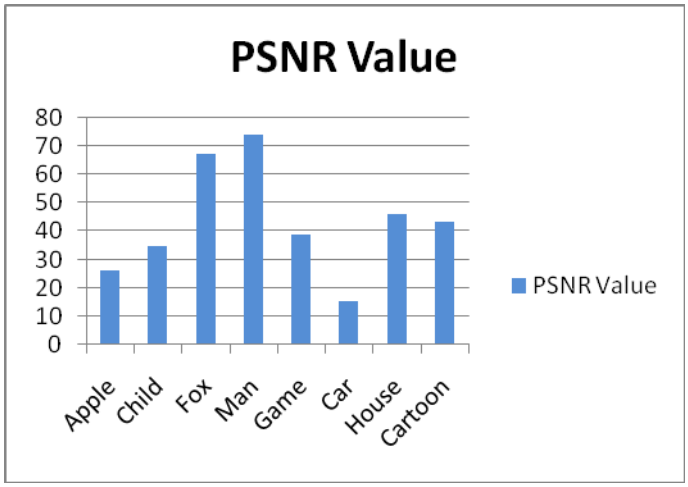


Fig. 1.4. PSNR comparison for different images

IV. CONCLUSION AND FUTURE WORK

Steganography is a interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. As steganography becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As

with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates, steganography and Steganalysis will continually develop new techniques to counter each other. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

The possible use of steganography technique is as following:

- Hiding data on the network in case of a breach.
- Peer-to-peer private communications.
- Posting secret communications on the Web to avoid transmission.
- Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

V. REFERENCES

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography Using Least Signicant Bit Algorithm” International Journal of Engineering Research and Applications (IJERA)

[2] Chao, H.-M., C.-M. Hsu and S.-G. Miaou (2002). "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records." Information Technology in Biomedicine, IEEE Transactions on 6(1): 46-53.

[3] Thien, C.-C. and J.-C. Lin (2003). "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function." Pattern Recognition 36(12): 2875-2881.

[4] Wu, H.-C., N.-I. Wu, C.-S. Tsai and M.-S. Hwang (2005). "Image steganographic scheme based on pixel-value differencing and LSB replacement methods." IEE Proceedings-Vision, Image and Signal Processing 152(5): 611-615.

[5] Yu, Y.-H., C.-C. Chang and Y.-C. Hu (2005). "Hiding secret data in images via predictive coding." Pattern Recognition 38(5): 691-705.

[6] Li, S.-L., K.-C. Leung, L. Cheng and C.-K. Chan (2006). "A novel image-hiding scheme based on block difference." Pattern Recognition 39(6): 1168-1176.

[7] EL-Emam, N. N. (2007). "Hiding a large amount of data with high security using steganography algorithm." Journal of Computer Science 3(4): 223.

[8] Yu, Y.-H., C.-C. Chang and I.-C. Lin (2007). "A new steganographic method for color and grayscale image hiding." Computer Vision and Image Understanding 107(3): 183-194.