International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 2, Issue2

Steganography for Colored Images

Mr.Pushparaj P.Nerkar, Vishwajit K. Barbudhe, Prof. Aumdevi K. Barbudhe

***Abstract* - In this paper, we present a novel method to embedding secret message in the cover-image. The basic concept of the proposed method is by simple Least Significant Bit (LSB) substitution. We propose a steganography method that applies a technique to embedding a wavelet compressed secret message within the Least Significant Bit (LSB) of the cover image pixels in a specific pattern. The proposed method results in increasing the secret message capacity and security level. The secret message won't be visible after embedding and can be extracted later.**

***Keywords* - LSB, Stegnography, Pixel, Capacity, Wavelet.**

I. INTRODUCTION

Ancient Steganography

The word steganography is originally derived from Greek words which mean "Covered Writing". It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew.

Back (Johnson & Jajodia, 1998), (Judge, 2001), (Provos & Honeyman, 2003) and (Moulin & Koetter, 2005). Steganography, the study of data hiding with the intent of sending a secret message, has become increasingly important over the last few years as the use of digital media, which provides ample space to hide the message, has become more popular. Generally, Methods of image steganography hide messages by using redundancy in the image. The message will be visually

Imperceptible as long as the insertion of the message does not cause any noticeable changes to the original image. Of course, it may be possible to detect the message using other means. The study of detecting secret messages is called Steganalysis. Each image hiding system consists of an embedding process and an extraction process. An innocuous-looking original image is used as the cover-image to conceal the secret data. The secret data are embedded into the cover-image by modifying the cover image to form a stego-image. Therefore, the embedding process may use an embedding key so that only the legal user can successfully extract the embedded data by using the corresponding extraction key in the extraction process. The embedding key and the extraction key are referred to as stegokeys.

In this paper, we present a new method which increases the secret message capacity and improves the quality of the cover image and security. The most important achievement of this work is a high PSNR level comparing to the existing method.

II. WAVELET

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. We use the DWT to implement a simple watermarking scheme. The 2- D discrete wavelet transform (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original; only on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low-pass and high-pass filters of the wavelet transform naturally break a signal into similar (low pass) and discontinuous / rapidly-changing (high-pass) sub signals. The slow changing aspects of a signal are preserved in the channel with the low-pass filter and the quickly changing parts are kept in the high-pass filter's channel. Therefore we can embed high energy watermarks in the regions that human vision is less sensitive to, such as the high resolution detail .bands (LH, HL, and HH).

III. IMPLEMENTATION

A). LSB (Least significant Bit) Substitution based Steganography:

Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB is:

$Xi' = xi - xi \bmod 2k + mi$ ---------- (1)

The ith pixel value of the stego-image and xi represents that of the original cover-image. Mi represents the decimal value of the ith block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in Equation (2).

$mi = xi \bmod 2k$ ---------- (2)

Hence, a simple permutation of the extracted mi gives us the original confidential data. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane.

b). Transform Domain based Steganography:

Robustness of steganography can be improved if properties of the cover image could be exploited. Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it. Different sub-bands of

frequency domain coefficients give significant information about where vital and non vital pixels of image resides.

Using transform-domain techniques it is possible to embed a secret message in different frequency bands of the cover. Embedding in the high frequencies creates less impact on the perceivability of the media but provide low robustness to different attacks. In contrast, embedding in the lower frequencies helps to withstand many attacks but creates perceptible impact on the media. So, middle frequency bands offers excellent location for data hiding. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in DCT or DWT.

c). Adaptive Steganography:

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" and "Masking". This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

IV. PROPOSED METHOD

A). Proposed Methodology of Solution

The proposed method in this project is to use a secret message which has the dimensions of 180*180 gray scale and will be embedded into a cover-image having dimensions of 512*512 RGB where the secret message will be wavelet Haar level 1 compressed then chose (LL) sub band and randomly codify it matrix, that this matrix should be kept somewhere for decoding that causes the safety to be increased. Then embedded into the bits of the cover-image .The secret message will be wavelet Haar level 1 transformed, then the difference coefficients of the wavelet transform will be quantized into 6 bit each .The result of transform will be a follows:

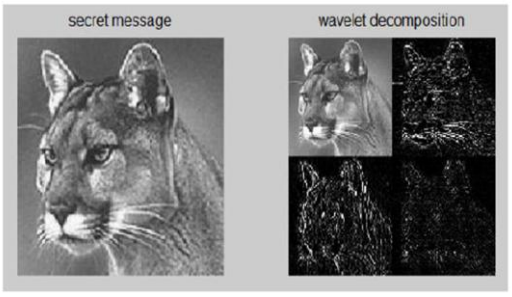


Fig. 1.Secret message and wavelet decomposition

b. The Embedding Procedure

Now we select a region of 360×360 pixels from the cover image. The (LL) sub band of the wavelet transform of the secret message is a 90×90 pixels image. Now each pixel is embedded in two pixels of the cover image as shown in Fig.3.1, so we need 16200 pixels and its embedding procedure is in Fig.3.2, it means that every pixel from the message image is embedded in 2 pixel of the main colored image. We use PSNR as a fitness function to evaluate the performance of each particle. The PSNR is defined as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{\frac{1}{(IH \times IW)}\sum_{i=1}^{IH}\sum_{j=1}^{IW}(O_{ij} - D_{ij})^2}\right)$$

Where Oij and D ij denote the pixel values of the secret message and cover image, respectively, IW and IH stand for the width and height of the cover-image, respectively.

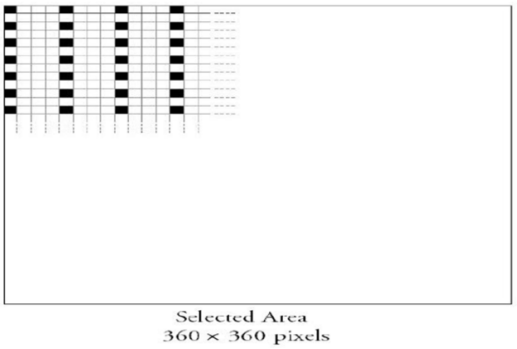


Fig.2.Selected area for embedding secret message into cover

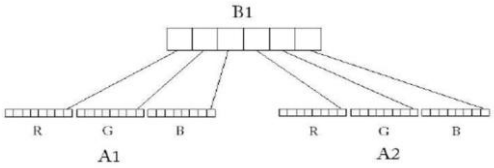
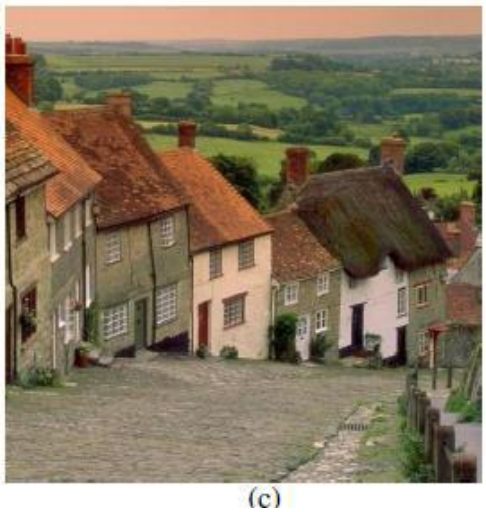


Image Fig.3. The algorithm used to embed each pixel in secret message into each 2 pixels from cover image

C. Experimental and Simulation Results

To evaluate the performance of the proposed technique, several experiments were conducted. In our experimental test, all cover-images were 512 gray levels, 512×512 in size. We chose the images "Lena", "Baboon" and "Goldhill" separately, shown in Fig. 4(a), (b) and (c), as cover-images and chose the image shown in fig.5, as secret message. We compared the experimental results of the proposed method to the ones of F.AL-Hunaity et al and if anyone succeeded to extract the message from the main image, it means that he/she has achieved the result shown in Fig.6. Now access to the main random matrix is essential to achieve the secret message and finding the random matrix is not a simple job. Therefore the security level is improved by the proposed method.

(a) (b)



(c)

Fig. 4.The cover images of our test data: (a) Lena, (b) Baboon, (c) Goldhill.

(a)

Fig.5. the secret message with 180×180 pixels

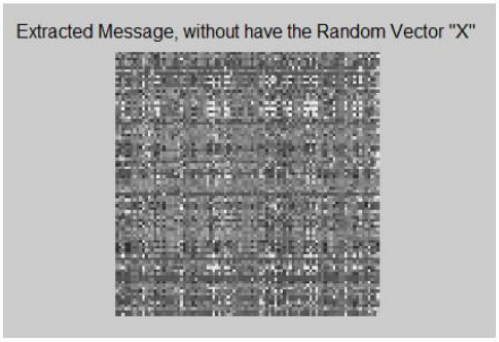


Fig. 6 Extracted message without have the random vector "x" We use PSNR as the secret message quality criteria to evaluate the performance of the methods. Calculated PSNR values are shown in Table 3.1. According to the results shown in Table.1. It can be seen that the quality of the proposed method is better than other methods.

		Images		
Method number	Method name	Lena	Baboon	Goldhill
1	Method of F.AL-Hunaity et al	58.4264	58.3878	58.4191
2	Proposed method	63.2532	63.2613	63.2214

TABLE 1. The PSNRs of the secret message (db)

V. ALGORITHM

This chapter discusses the basic algorithm to embed a message in an image using the singular value decomposition. The algorithm for extracting the message is also discussed in this chapter. In this project, I have implemented Image steganography using two platform one in Matlab and other in Android. In both we are Converting RGB image or color map to rayscale by eliminating the hue and saturation information while retaining the luminance. In Matlab, cone shape is intersected on 8 bit planes of image, than shift operation is performed on the image. In Matlab module we are reading text file to hide behind the message and in Android module we are reading text file from resource folder and selecting image from photo gallery to use as cover object to hide. The message is also converted into bytes and is inserted at intersection of geometric objects points and pixels of image. In Matlab, I have used cone as geometric object for hiding message in image and for android module polygon name hexagon is used. I have tried the combination of Steganography and cryptography for hiding message by encrypting with AES algorithm to provide better security and more complexity.

Flow of Encoding Mechanism for Matlab:

In the previous chapter, we saw how images are converted into grey scale image than image is divided into 8 bit planes. In Matlab Module, Color image is initially converted into grey

Scale image. This grey scale image is used as an input to the steganography. A bit plane of grey scale image is set of bits having the same position in the respective binary numbers. For

Example, for 8-bit data representation there is 8 bit-planes: the first bit-plane contains the set of the most significant bit and the second bit-plane contains the second most significant bit and so on. All these image bit planes are shifted by 1 bit and then cone is inserted into these 8 bit planes. Intersection point of cone and image are then considered as a place where sender has to hide his secret message. So the recipient of message can find the hidden message.

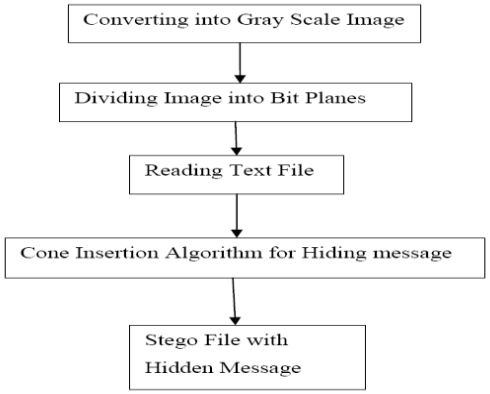


Fig.7. Flow of encoding image steganographic Process in matlab

Decoding of steganography messages:

The message is decrypted using AES algorithm. Decryption is the reverse process of encryption that is getting original data back from encrypted message. To decipher the message, the receiver of the encrypted data must have the proper decryption key (password) as AES is symmetric key or private key cryptography.

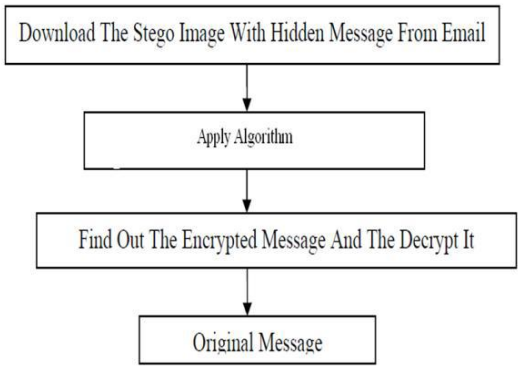


Fig.8...Flow of decoding image steganographic

Decoding Text in Matlab Module:

A bit plane of a digital image is a set of bits having the same position in the respective binary numbers. For example, for 8-bit data representation there is 8 bit-planes: the first bit-plane contains the set of the most significant bit and the second bit-plane contains the second most significant bit and so on. In the decoding process the gray scale image is converted into 8-bit planes. All these image bit planes are shifted by 1 bit and then cone is inserted into these 8 bit Planes. Intersection point of cone and image are then considered as a place where sender has hide his secret message. So the recipient of message can find the hidden message.

VI. RESULT

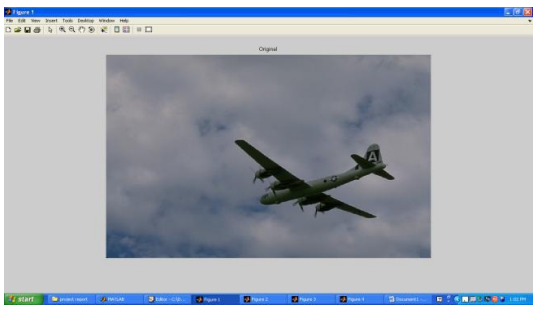


Fig.9.Original Image

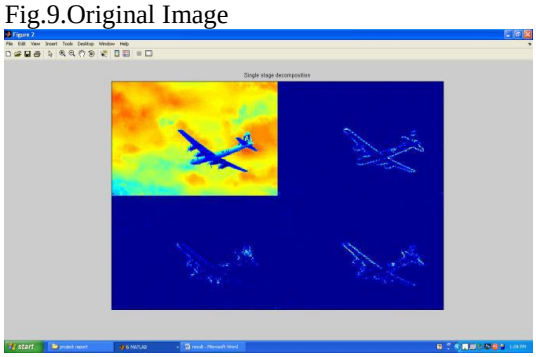


Fig 10.Single Stage Decomposition Image

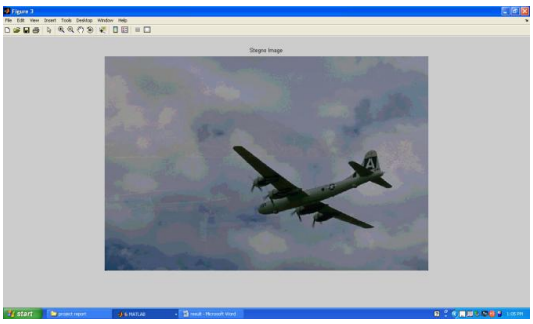


Fig 11.Stego Image

Fig12.Extracted Image

Sr.	Calculation	Result
1	Compression ratio	0.9625 db
2	SNR	24.89 db
3	PSNR	29.92 db
4	MSE	66.16 db

Table 2. Calculated Result for above images

VII. CONCLUSION

As far as data hiding using steganography is concerned, two primary objectives are interesting: the technique that will be used for steganography should provide the maximum possible payload, and the embedded data must be imperceptible to the observer. It should be stressed on the fact that steganography is not meant to be robust. Any modifications to the file, such as conversions between file types, standard image processing (compression, filtering, .etc.), or geometrical editing (rotation, resizing, cropping, etc.,) are expected to affect (and may remove) the hidden bits from the file. The proposed method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. Then, it uses Wavelet transform to transform both the cover image and the hidden message. Wavelet transform allows perfect embedding of the hidden message and reconstruction of the original image. Steganography is powerful and effective for communication of secret data. In some countries, cryptography is not allowed to be applied in full application.

They have put certain restrictions due to security reasons. Steganography is very important in such situations. On the other side, steganography alone is not secure entirely. Steganography when combined with cryptography indeed becomes a powerful method of secure of communication. Finally, steganography subject is still young, not mature, and the work on it will continue to increase the Capacity, security, and robustness. Since these factors contend with

each other, the new methods will try to make the best trade-off.

Limitations:

To validate in Matlab Module, we have already mentioned name of cover image to be used in code and text file name to be read. In Android module, message from text file is made to read and cover image is selected from picture gallery available in that particular SD Card. In my application all images has to be jpeg file and for android application has to be of at least 1024x768.The memory card is basic requirement for Android otherwise application would not execute further. Sometimes Downloading Larger images from gmail forces android phones to stay in busy mode. So my suggestion is to attach embedded image manually with email.

Future Enhancements:

The existing application is a desktop application. The Java application runtime (.jar) that is created using the eclipse IDE which is nothing but an archive which can be moved to any workstation irrespective of the operating system that the workstation has and a single click can easily install the entire system on the respective machine. Google wants to protect its phone users from installing and running fraudulent software on their devices. Therefore, each and every application needs to be signed with a valid certificate that ensures where the application comes from.

VIII. REFERENCES

[1] Anjali A. Shejul, Umesh L. Kulkarni "*A Secure Skin Tone based Steganography Using Wavelet Transform* "International Journal of Computer Theory and Engineering, Vol.3, No.1, 1793-8201 ,IEEE February 2011

[2] Adel Almohammad and Gheorghita Ghinea Brunel University *"Stego Image Quality and the Reliability of PSNR",* 1-6, IEEE 2010

[3] Saeid Fazli, Sajad Gholamrezaei *"Advanced Wavelet Based Steganography for Colored Images",* International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 377-380, IEEE 2010

[4] MohammadReza Keyvanpour," *A New Encryption Method for Secure Embedding In Image Watermarking* ", V2, 403-407, IEEE 2010

[5] Chang GAO, *"Image Authentication Method Based On DWT in Color JPEG Images",* International Conference on Environmental Science and Information Application Technology, 370-374, IEEE 2009

[6] Ankur Dauneria, Kumari Indu," *Encryption Based Data Hiding Architecture with Text Pattern Authentication and Verification*"236-241, IEEE2008

[7] Vinay Rishiwal, Hirdesh Kumar*," Multiple Secret Images Sharing Scheme",* 1-4, IEEE 2008

[8] Mamta Juneja," *Designing of Robust Image Steganography Technique Based onLSB Insertion and Encryption*", 302-305, IEEE 2009

AUTHOR'S PROFILE

Pushparaj Pundalikrao Nerkar
Electronics and Communication Engineering Technocrats Institute of Technology, Bhopal R.G.P.V, Bhopal. (M.P)
Email id: nerkar.pushpak@gmail.com mob. No .08600992134

1) International conference at Dhule, paper present on "Stegnography for Color Images".
2) International conference at Navalnagar, paper present on "Novel Optical fiber cables using ultrahigh rensity".
3) National conference at Nashik, paper present on "Optical fiber Pressure transducer use in upper airway.

Mr. Vishwajit K. Barbudhe,
CDAC , M.Tech in EC Engineering (Pursuing), Department of E&TC , TIT College of Engineering,RGPV University ,Bhopal, India ,9028291182
Email:vishwajit.k..barbudhe@gmail.com

1) Holographic memory, National level technical symposium technizzma-10 Shree Hanuman Vyayam Prasarak Mandal's, College of Eng. &Tech. Amravati
2) Image processing, G.H. Raisoni College of Engineering and Management, Amravati
3) Importance of Legal Literacy in Growth and Development of India. National conference on role of education, physical education and sports to make India super power2020 Dr Babasaheb nandurkar collage of physical education yawatmal

Aumdevi K. Barbudhe,
Assit. Prof.
MSC Computer Science, Department of Computer Science and Technology, Dr.BNCPE College, Amravati University, Yavatmal, India. E-mail:bhavana.barbudhe@rediffmail.com, 9970909262

1) Data Warehousing and OLAP technology
National conference on futu ristic computer application Sponsored by: university of Pune .All India Shri Shivaji Memorial Society's, Institute of Information Technology, Pune.
2) Mobile Computing, National level technical symposium technizzma-10 Shree Hanuman Vyayam Prasarak Mandal's, College of Eng. &Tech. Amravati
3) Cloud computing, G.H. Raisoni College of Engineering and Management, Amravati
4) Importance of Legal Literacy in Growth and Development of India. National conference on role of education, physical education and sports to make India super power2020 Dr Babasaheb nandurkar collage of physical education yawatmal