ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2014,
Vol. 7, No. (3):
Pgs. 358-362

A Novel Secure Image Hiding on Indexed Images using Pixel-Matching Technique

J.N.V.R.SWARUP KUMAR and CHAITANYA VEMALI

Department of CSE, Gudlavalleru Engineering College, India.

(Received: November 10, 2014; Accepted: December 20, 2014)

ABSTRACT

Steganography is the science of hiding the fact in the information which we are sending. The goal of steganography is to embed a secret message inside a piece of unsusceptible information. The result of steganography depends on the secrecy of the cover carrier. After the steganographic carrier is disclosed, the security depends on the robustness of the algorithm and the cryptographic methods used. In order, to achieve secrecy, either the carrier must be made more robust against steganalysis or new and better carriers must be discovered. The main intention behind this paper is to discuss a new steganography technique for indexed images.

Key words: Steganography, Cryptography, LSB, Pixel-Matching, Indexed Image, Steganalysis.

INTRODUCTION

Steganography means covered or hidden writing[1, 3]. The goal of steganography is to send a message through some unsuspicious carrier. The message can be a text, an image or it can be an audio file. Steganography technique helps in hiding the fact that a secret message is being sent in original information. Digital steganography is a technology used for changing the digital carriers such as images or sounds. These changes are made to hide the secret message, but the successful results should not affect the carrier.

Steganography methods combine many aspects of digital signal processing, cryptography, statistical communication theory and human perception. Cryptography is not similar to steganography. Cryptographic techniques are used to scramble a message so that it cannot be read by a third party, the attacker. If at all a cryptographic message is discovered, it is difficult or impossible to understand and de-code it, since the message is encoded in human unreadable format. Steganography hides the very existence of a message in the cover medium. It is a good practice to encrypt a message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that the secret information has been exchanged. Furthermore, if an attacker were to defeat the steganographic technique and detect the message from the stego-image, he would still require the cryptographic decoding key to decipher the encrypted message.

Segmentation is the process of partitioning a digital image into multiple segments. Using segmentation, we can simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to consider desired part of the image. More precisely, image segmentation is the process of assigning a label to every pixel in an image where the pixels with same label share certain visual characteristics.

Background theory

In the last few years, the theoretical foundation of information hiding has advanced very rapidly. Modeling the information hiding process as one of the secured communications improved information hiding algorithms as well as accurate models of the channel capacity and error rates. At the same time, steganography security, i.e. the ability of information hiding to serve in a scenario where an enemy explicitly aims at nullifying the hidden information goals, whatever they are, has been recognized as one of the main open issues in implementing this technique.

As explained in reference[10], for all the steganographic systems, most vital and elementary requirement is the undetectability. The hidden message should not be detected by other people. Moreover, the cover message with hidden message i.e. stego-media is indistinguishable from the original ones i.e. cover-media. The cover-media and stego-media should appear identical under all possible statistical attacks and meanwhile the embedding process should not degrade the media fidelity[8] Presents several attacks on cover media.

Table. 1: Comparative Results

S.No	Original	Regular	Embedded
1	71.2131	71.2107	71.2133
2	91.4541	91.4515	91.454
3	116.8887	116.8766	116.8881
4	82.7183	82.7076	82.7182
5	131.8025	131.799	131.8025
6	101.9898	101.9865	101.9898
7	105.4361	105.4215	105.4353
8	91.9313	91.9226	91.9305
9	18.9911	18.9803	18.9914

The difference between stego-media and the cover-media should be imperceptible for visual attacks.

Steganography uses two types of protocols: secret-key and public-key steganography. In secret-key steganographic model, both sender and receiver share a secret-key before conveying messages. The input message may be in any digital form and be treated as a bit stream. Public-key cryptography requires the use of two keys, one private and one public key. The public-key is used in the embedding process whereas the private key is used in extracting the hidden message.

Even though a considerable number of steganographic techniques were in use, study of this subject in the scientific literature goes back to Simmons[5], who in 1983 formulated it as the “prisoners’ problem”. A detailed review on steganographic techniques is discussed by the author in her previous paper Ref[2].

Digital Steganography Methods

The steganography applications range from those that actually hide data, often encrypted, within the file, to those that simply attach hidden information to the end of a file such as Camouflage. As explained in Ref. [7], the community is concerned with a number of digital technologies, namely, text files, images, movies and audio. One of the main methods typically used for steganography involves the process of hiding a message in image pixels. Digital images are the most widespread carrier medium used[9]. Neil F. Johnson[6] explains different methods of hiding data in digital images.

Image-based Steganography

Many steganographic tools are available in the internet for varied image formats. The fact that images can be subjected to lossy compression methods has suggested that extra information could be concealed in them. Properties of images including luminescence, contrast and colors can be manipulated. A 24-bit color image has three components corresponding to Red, Green and Blue. The three components are normally quantized using 8 bits. An image made from these components is described as a 24-bit color image. Each byte can have a value from 0 to 255 representing the intensity of the color. The darkest color value is 0 i.e; black

and the brightest is 255 i.e. white, Transparency is controlled by the addition of information to each element of the pixel data. A 24-bit pixel value can be stored in 32 bits. The extra 8 bits are used for specifying transparency. This is sometimes called the alpha channel. An ideal 8-bit alpha channel can support transparency levels from 0 (completely transparent) to 255 (completely opaque). It can be stored as part of the pixel data. Structure of digital images is discussed in the *"An evaluation of Image Based Steganography Methods"* by Kevin Curran of Internet Technologies Research Group[9].

Current techniques for embedding messages into image carriers fall into three categories[4,7]:

- Least-Significant Bit embedding (or simple embedding)
- Transform techniques.
- Perceptual masking & Filtering Techniques.

The proposed method

This methodology uses indexed (24 bits/ pixel) bitmaps such as BMP, GIF & PNG as the carrier medium to hide secret images. The bits of secret image will be hidden inside the indexed image. High secured applications are resulted by using steganography technique. Now each pixel of carrier image will be replaced by image pixels which are to be embedding with respective color codes.

This new pixel matching technique can be used with all the types of color images. As the pixel matching technique allows embedding a whole character into a single pixel, more data can be embedded in the image.

This piece of work discusses about a tool that will not only work on 24 bit indexed color images but also be able to encrypt the secret text using asymmetric key cryptography and hide secret text messages inside the selected segment of image.

The techniques used for the proposed method is explained in the following steps:

Hiding Image in the Image

The following are required for hiding a message:

1. A carrier image (color)
2. Secret message in image format
3. Dictionary file.

Extracting a Hidden Message

Extraction process shown in figure2 is much easier than hiding. The dictionary file is required to locate a carrier pixel. Pixel can be checked for the image and the bits found in the RGB components are saved. This process will be continued until the image is completely found.

Algorithm for Proposed Method

Steps to Hide the Image Using the Proposed Method:

1. Choose the proper image for the cover medium.
2. Identify the color value of pixels.
3. Choose the appropriate pixel value of carrier image and replace with the embedded image

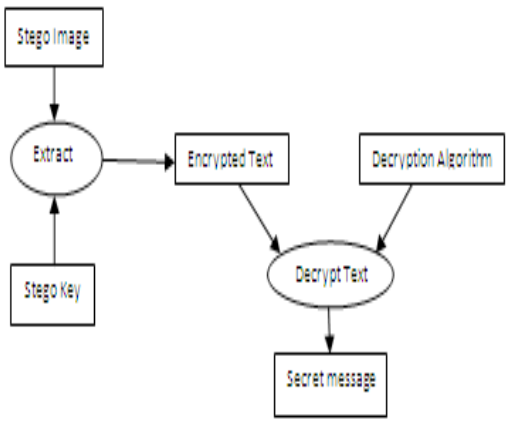

Fig. 1: Hiding Image in the Image

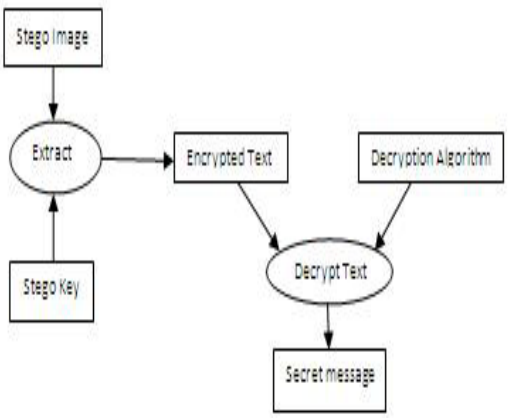

Fig. 2: Extracting the Hidden message

pixel value.

4. If there are no equal pixel values then those will be replaced by nearer pixel values.
5. Store the locations of embedded pixels in dictionary file.
6. Send the stego image to the destination.

Steps to Extract Image Using the Proposed Method:

1. Select carrier image which is received.
2. Select the appropriate pixel value of stego image based on the dictionary file.
3. Construct secret image from the extracted stego image pixels.
4. After extraction, the secret image message is available to use.

Experimental analysis

The traditional LSB methods do not provide high capacity and flexibility to hide a whole character/ pixel in a single pixel. Usually steganography is applied for normal images. By using the proposed pixel matching technique, we can provide high level security to the secret message against steganalysis.

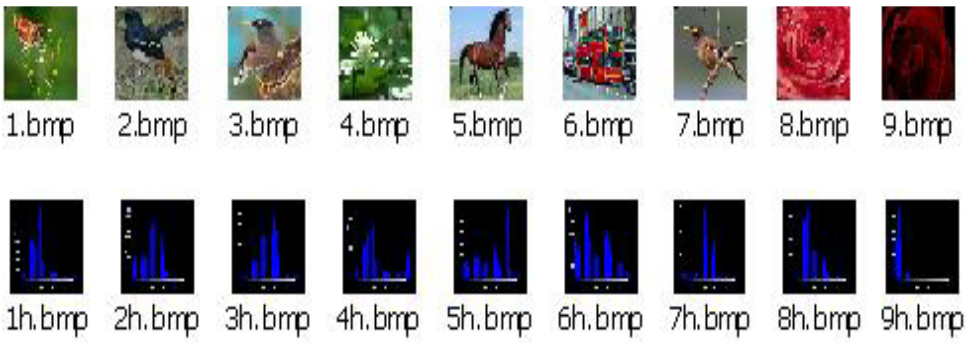

Fig. 3: Original Images and its Histograms

Fig. 4: Regular LSB Embedded Images and its Histograms

Fig. 5: Proposed Pixel-Matching embedded Images and its Histograms

By using this, proposed method provides better security compared to steganography that is usually used to hide the normal text and image. As a whole, the analysis shows that the performance of the proposed method is much better than the existing methodologies

The above results point up that the mean of proposed method values increased than original and regular LSB methods. When a message is embedded in the image by using regular LSB method, message bits are stored in pixels eight bit plane. Thus, the pixel value does not change well. Hence the mean value of image has not changed much and the value is relative to original image mean. When a message/image is being embedded in the image by using proposed Pixel-Matching method, message bits of single character are stored in a single RGB pixel. So, pixel value does not change than other embedding methods. Despite mean value of proposed method increases integrity of message and enhances sturdiness of application security. In total, the analysis shows that the performance of the proposed method is much better than the current methodologies.

CONCLUSION

In this paper we have presented a new modus operandi of adaptive steganography with higher embedding capacity using Pixel-Matching technique on indexed images. The embedding capacity of this approach is very high. What's more is, this method is to a considerable extent robust with the use of Pixel-Matching technique. By using this novel secured mechanism for steganography, we can provide security to cloud applications like secured data transmission, session management and etc.

REFERENCES

1. A Discussion of Covert Channels and Steganography by Mark Owens, March 19, (2002).
2. Review on current steganography technologies by S. G. K. D. N. Samaratunge, 7th International Information Technology Conference, Sri Lanka (2005).
3. An efficient color re-indexing scheme for palette based compression by Wenjun Zeng, Jin Li and Shawmin Lei, Sharp Laboratories of America.
4. A Review of Data Hiding in Digital Images by Eugene T. Lin and Edward J. Delp, Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, Indiana.
5. On the limits of Steganography by Ross J. Anderson, Fabien A. P. Petitcolas, IEEE Journal of selected areas in Communications, 16(4):474-481, May 1998. Special issue on Copyright & Privacy protection. ISSN 0733-8716).
6. Exploring Steganography: Seeing the Unseen by Neil F. Johnson, Sushil Jajodia, George Mason University.
7. Steganography and the Art of hiding information by Vish Krishnan, Overland Park, K.S.
8. Information hiding – a survey by Fabien A. P. Petitcolas, Ross J. Anderson & Markus G. Kuhn (Proceedings of the IEEE – special issue on protection of multimedia content, 87(7):1062-1078, July 1999).
9. An evaluation of Image Based Steganography Methods by Kevin Curran, Internet Technologies Research Group, University of Ulster Karen Bailey, Institute of Technology, Letterkenny, Ireland (International Journal of Digital Evidence).
10. Secure Error-Free Steganography for JPEG Images by Yeuan- Kuen Lee, Ling-Hwei Chen, Department of Computer and Information Science, National Chiao Tung University, 1001 Taiwan, R.O.C. *Second international Conference on Industrial and Information Systems,* ICIIS 2007, 8 – 11 August 2007, Sri Lanka 339.
11. New Steganography Technique for Palette Based Images by S.G.K.D.N. Samaratunge, University of Colombo School of Computing (UCSC), University of Colombo, *Second International Conference on Industrial and Information Systems, ICIIS* 2007, 8 – 11 August 2007, Sri Lanka.