Middle-East Journal of Scientific Research 23 (2): 357-361, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.02.22127

Security Enhancement in Image Steganography a MATLAB Approach

M. Kameswara Rao, K. Pradeep Reddy and K. Eepsita Saranya

Department of Electronics and Computer Science K L University, Vaddeswaram Andhra Pradesh, India

Abstract: Steganography helps in communication of secured data in several carries like images, videos and audio. It undergoes many useful applications and well known for ill intentions. It was mainly proposed for the security techniques in the increase of computational power, in order to have security awareness like individuals, groups, agencies etc. The factors that are separated from cryptography and water making are data is not detectable; capacity of hidden data is unknown and robustness of medium. The steganography provides different methods existing and guidelines. The current technology of image steganography involves techniques of LSB in image domain but once the attacker acknowledges that medium is containing embedded data he will attack the medium and breaks into the secured content. In this paper we are discussing how to protect the steganography image by embedding it into another medium using mat lab. Here we work on image matrices to perform the steganography. Lightness adjustment on the matrix is done to reduce the brighter pixels in image. The lightness decreased image then embedded into another cover image by matrix difference technique (will be discussed in detail). This enhances the security to a higher level because to acquire the steganography image embedded we need to have the key image which will be having only by the receiver. And from millions of images on the internet it is impossible for an attacker to guess the key image. And this enhances the level of security.

Key words: Steganography · LSB · MATLAB · Image Processig · Cryptography

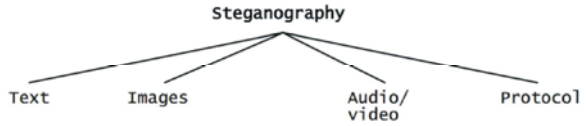
INTRODUCTION

Steganography is an art of hiding information, this word originated from Greek in which Steganós means Covered and Graptos means writing that literally means "cover writing" [1].

Since everything is computerized these days and all the data is transmitted and shared through internet, we need to have security of higher orders to protect the confidential data. Thus we need cryptography and steganography concepts the drawback of cryptography is it will be known that we have encrypted data and well before and people starts to crack it. But in the case of steganography it's not possible to know that there is data embedded into a medium. If there is a large stream of medium audio, video, image) it's not possible to guess which contains the embedded data. It is quite different from cryptography where cryptography helps in keeping the message as a secret where steganography helps in keeping the existence message as a secret among neither of it is perfect. If the data hidden was revealed, then the steganography is slightly defeated. The security can be increased by the combination of cryptography. Another two technologies namely watermarking and fingerprinting are nearer to stenography but has different requirements. In those two techniques the hidden information can be visible, but in steganography the information is crucial. A successful attack of stenographic system has an advanced observation of information hiding inside the file, whereas the fingerprinting and watermarking techniques cannot have the capability of detecting the mark. The realization of potential with respect to steganography in new product information was also started in the business. The leakage of information can be avoided by communicating with well-known channels. Hiding the information in the form of photographs can be less suspected than communication. This paper helps us to know about the overview of different algorithms used for security purpose in steganography both in business and personal use.

Corresponding Author: M. Kameswara Rao, Department of Electronics and Computer Science, K L University, Vaddeswaram Andhra Pradesh, India.

Different Kinds of Steganography: Almost every digital file can be employed for performing the steganography, formats with a high degree of redundancy are more helpful. Redundancy means bits of an object/a file that provide accuracy to it far better than necessary for the object's use and display for example if we have a photograph of clear sky most of the pixels in the image are in blue they are considered are redundant pixels in this case all those unnecessary pixels are defined in the matrix are defined a number of times, but in fact not necessary so they are called the least significant bits. These redundant bits of can be altered without the without creating a visible distortion in the final image. Image and audio files especially meet this required criterion. Figure below shows the four main categories of file formats that are used in current steganography technology.



Text Steganography: In the text steganography the number of tabs or white spaces or capital letters are used for achieving the steganography, just like Morse code [2] and etc. is used to achieve information hiding.

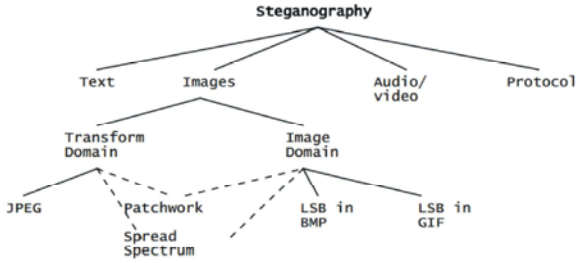
Video Steganography: Video (series of pictures w.r.t to a timeline) is used as medium for Hidden information. The values in the Discrete Fourier Transform are manipulated, which is not Noticeable to the human eye. Video steganography can be done on the formats such as H.264, Mp4, MPEG, AVI etc.

Audio Steganography: It became very familiar due to the growth of the Voice over Internet Protocol (VOIP) popularity. Audio steganography can be performed on the digital audio formats such as WAVE, MIDI, AVI, MPEG etc.

Protocol Steganography: In general networking a protocol is used as carrier and if such protocol is used for steganography then it is known as network protocol steganography. In OSI reference model we have covert channels where we can achieve the steganography in unused header bits of TCP/IP fields [3].

Typical image steganography is categorized in following aspects [4] High Capacity, Robustness, Temper Resistance, Computation Complexity. Image steganography broadly classified into two families; Image domain and Transform domain. Image also known as spatial, domain techniques embed messages in the intensity of the pixels directly, while for transform, also known as frequency domain, images are first transformed and then the message is embedded in the image this makes the transform domain secured little extent more than image domain.

The image steganography further divided into these fallowing categories based on the technique applied for the process.



The most familiar technique employed in the steganography is LSB in BMP images bitmap images are not optimized in size like JPEG so there is chance of having higher redundant pixels and in turn we have least significant bits making this process more reliable for steganography.

Most of the digital files having the degree of redundancy can be used in steganography. Redundancy means the object bits that provide more accuracy for objects use and display than the required content, these bits can be altered without being detected easily. Generally image and audio files will comply with the above requirement. Information hiding plays an important role in steganography. As text files have small redundant data is not used very often in text steganography. Hiding information in images is focused in this paper. In internet the more amount of redundancy bits present in the representation of a digital image are the most popular cover objects for steganography. Similar techniques for both image and audio files take place in hiding the information. Audio steganography in masking is the different technique, which explodes hiding information of the human ear unnoticeably (in this case the sound that was audible becomes inaudible). Steganography generally refers to the technique of information embedding within the messages and the network protocols used in the network transmission. The steganography can be used in OSI network model of converting channels. Image steganography is widely used because of the frequency of images is increased due to the social networking at an average 40 million new images are uploading to the internet per week.

Related Works: Neil F. Johnson, Sushil Jajodia *et al*. [5], Has discussed different masking and filtering techniques of steganography and compression of the files.

Piyush marwaha, paresh marwaha [6], They put forward the concept of multiple cryptography in which the data will be encrypted into a cipher in stage one and the cipher will be hidden into an image file.

Mamta janesa, parvinder sing sandhu *et al*. [7], They gone through the LSB insertion & RSA encryption technique dsusing the a robust image steganography technique.

Feng Pan, Jun Li *et al*. [8], They presented horizontal pixel & vertical pixel difference utilization algorithm, in the horizontal direction they use high quality model function method for two pair of pixel embed message they use PVD method.

Westfielda & Pfitzmann [9], They proposed a particle algorithm for embedding Joint Photographers Experts Group(JPEG) image that would provide a greater capacity without sacrificing security.

Ming. Chen, Z. Ru. *et al*. [10], They explained several tools to hide the information within an image. All such tools are basically classified into five category on their algorithm i.e are spatial, transform, document, file structure, video compress encoding and spread spectrum.

Mehdi Hussain and Mureed Hussain [11], in this paper different forms of the steganography are discussed Image, Network, Audio, Video and text steganography are discussed and summarized the 9 spatial domain techniques that are used in the image steganography from which we used the LSB in spatial domain. Also discussed techniques in transform domain applied on the image.

James C. Judge [12], this paper briefly stated, Definition of steganography on which steganography can be performed. And number of processes that will hide a message within an object that are available currently, where the hidden message will not be apparent to an observer. This paper explored steganography from birth to till date and the future scope of steganography.

Existing Technology: The current technology is the combination cryptography and steganography. The content in the medium is protected in this technology but the medium is not protected this makes it easy to intrude into and makes the content to be exploited easily. There is no technique to protect the medium explicitly.

Proposed Technology: Here we are proposing a technology to protect the carrier medium so that the chances of guessing the medium contains data is minimal.

Description: In image steganography by LSB method we predict the least significant bits in the image which are raised to repetitive patterns in the digital images and we place the cipher or plain text content into those bits so that the output image is un distorted or with minimal distortion if the process carried out un ideally. But the image containing text is not protected, out method will carry out the process of protecting the medium the image is protected by steganographing into another image. It is carried out by either Adobe(R)Photoshop(TM) v11 above or Simulink(R) Mat Lab(TM) V 2010 a above. This process is carried out in two steps

- Generating the darker version of the image to be hidden (Decreasing the lightness).
- Generating the differential image matrix of darker image and the Cover Medium. In this method to obtain the required hidden image we need the undistorted cover image is key. Image as key method enhances the security to very high level. The decoder needed to have the key image else obtaining image is near impossible, it is impossible to guess the key image from the stream of millions of images over the internet.

Protecting the Cover Medium:

- Generating the darker version of the image to be hidden:

All the images in the RGB (not dealing with CMYK in this method) will have the matrix structure and for every pixel (square or round) we have the values for Red, Green and Blue. From the fact that Red, Green and Blue are the primary subtractive colors. Every pixel will have the RGB(0,0,0) to RGB(255,255,255) where RGB(0,0,0) is black and RGB(255,255,255) is white. And all the color in between are spread over the visible spectrum of colors 16.8 million (16777216) colors to generate the darker version of the image we can perform two operations

Decreasing the Lightness of the Image

Decreasing the RGB Range: Both methods do nearly same work making the RGB high value to (<255, <255, <255) so that there will be no brighter pixels in the image. In mat lab in order to Decrease the RGB high limit we need divide the matrix by approximately 15 or get approximately 8% of the original pixels so that the resultant image matrix the white pixel RGB (255,255,255) will Become RGB (15, 15, 15) approximately.

darkerImage = |imageToBeHiden/15| or
= |imageToBeHidden*8%|

- Generating the differential image matrix of darker image and the Cover Medium:

We need to consider relatively brighter image as the cover medium. To generate the differential image matrix the fallowing equation is applied.

resultImage = |imageToBeProtected-coverImage|

AS the cover medium is sufficiently brighter when the image to be hidden in darker version is subtracted there is not much visible disturbance in the image is observed. And this image will be transmitted to end user.

Un-Hiding Algorithm:

- For un-hiding the image we need to acquire final image and undistorted cover image as key.
- Darker version of the hidden image is acquired by calculating the difference of the final image and the undistorted cover image.
- The original can be obtained by multiplying the image back by 15 or approx. 830% of the darkened image.

darkenedHiddenImage = |finalImage ~ originalCoverImage|

HiddenImage = |darkenedImage *15| or
= |darkenedImage *1500%|

RESULTS AND DISCUSSION:

This is a BMP image this is used for LSB technique steganography using the current existing method.

The least significant bits in the bitmap matrix are manipulated and the required cipher text in inserted in to the image. Now a new method to secure this image is implemented in order to do this the image needed to darken using the techniques described in the paper above.

The steganography image is then subjected to darkening gives the below result.

When this Bitmap image darkened every pixel from the range of 0-255 in each spectrum of color will be reduced down to 0-15 this gives the darker version. Can be achieved by either mat lab of Photoshop. We used mat lab 2014a and image processing tool box for image functions in it.

Protecting the Steganography Image: For protecting this image we need to use another image to hide this image into that image. The target image must be considerably brighter so that when we calculate the difference the output shouldn't have considerable distortion.

The final output image (Difference of darkened image and cover image looks as below).

The final output image looks almost similar to the original cover image as the cover image is containing most pixels bright. This image contains the steganography image that contains the cipher text.

And for obtaining the hidden image we need the original cover Image as the key for revealing.

This completes the process of securing the image in another cover image. And to get the hidden image back we need two images the final image and original cover image which acts as key.

*As huge image is processing is involved in every step the time complexity of the algorithm will be considerably high.

There is chance of losing the originality of the image because the RGB matrix store only integers.

During the transmission the resolution of final image and cover image should not change, else the total Least Significant Bits will be disturbed destroying the image.

REFERENCES

1. Pfitzmann, B., 1996. Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp: 347-350.
2. Johnson, N. and S. Jajodia, 1998. Exploring steganography: seeing the unseen, IEEE Computer, pp: 26-34.
3. Handel, T. and M. Sandford, 1996. Hiding data in the OSI network model, Proceedings of the 1st International Workshop on Information Hiding.
4. Lin, E. and E. Delp, 1999. A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, pp: 25-28.
5. Johnson, N.F. and Sushil Jajodia, 1998. Exploring Steganography: Seeing the Unseen, Survey Paper, IEEE-1998.
6. Piyush, Marwaha and Paresh Marwaha, 2010. Visual Cryptographic Steganography in Images, Second international conference on computing, communication and networking technologies.
7. Mamta Juneja and Parvinder Singh Sandhu, 2009. Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, ICARTCC.
8. Feng, Pan and Jun Li, 2011. Image Steganography Method Based on PVD and Modules Function, IEEE-2011.
9. Pfitzmann and A. Wesrfeld, 2000. High Capacity Despite Better Steganalysis, Kluwer Academic Publisher Boston Dodrecht London.
10. Ming, Chen and Z. Ru. N. Xin, 2006. Analysis of Current Steganography Tools: Classification & Features, Information Security & Tele. Comm. Beijing.
11. A Survey of Image Steganography Techniques; Mehdi Hussain and Mureed Hussain, 2013. IJAST, pp: 54.
12. Steganography: Past, Present, Future; James C. Judge GSEC Version 1.2f www.sans.org/reading-room/whitepapers/stenganography/steganography-past-present-future-552.