Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.261 – 270

A Novel Algorithm for RGB Image Steganography

Mr.C.Thiagarajan[1], Ms.N.Aarthi[2], Ms.R.Ananthi@Valli[3], Ms.R.Anitha[4], Ms.A.Ruthira[5]

[1]Assistant Professor (ECE) Sri Ganesh College of Engineering and Technology, Puducherry

[2345] B.Tech (ECE) Sri Ganesh College of Engineering and Technology, Pondicherry

vcrajan99@gmail.com, r.ananthi.023@gmail.com, smranitha18@gmail.com, ruthira.ammai@gmail.com

Abstract: In steganography, the total message will be invisible into a cover media such as text, audio, video and image in which attackers don't have any idea about the original message that the media contain and which algorithm use to embed or extract it. In the proposed technique, a new steganography technique is being developed to hide large data in Bitmap image using filtering based on algorithm, which uses MSB bits for filtering purpose. This method uses the concept of status checking for insertion and retrieval of message. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images. It is being predicted that the proposed method will able to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. It efficiently and effectively hides data with the help of a key in RGB colored digital image. Proposed algorithm is capable to hide more data in cover image and require no pre-processing. Image Steganography is one of the common methods used for hiding the information in the cover image. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Results show that there is less detectable distortion in the stego image and opens the track for proposed algorithm to be used in data hiding and secure transmission.

Keywords - Steganography, Information Hiding, Pixel Mapping, RGB Image, Cover Image, Method, Optimal Substitution, Stego Image

I. INTRODUCTION

Since man first started communicating over written messages, the need for secrecy was in high demand. In the past, messages could easily be intercepted and since there were no secrecy devices, the third party was able to read the message. This all changed during the time of the Greeks, around 500 B.C., when Demaratus first used the technique of Steganography. Steganography is the use of hiding a message so it looks like a message does not exist at all. The official definition, according to Dictionary.com, is hiding a secret message within a larger one in such a way that others cannot discern the presence of contents of the hidden message. Steganography is the art of hiding information within innocuous cover carriers in ways such that the hidden message is undetectable. In Greek, 'stego' means 'covered' or 'secret' and 'graphy' means to ‘write’ and therefore , steganography becomes “covered or secret writing”. The information to be hidden is embedded into the cover object which can be a text matter, some image or some audio/video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resulted object exactly same as the original. The main goal of steganography is to hide that fact the message is present in the transmission. A majority of the messages hidden today are hidden inside digital images, audio files or video files.

Types of Steganography:

1) Text steganography: It is not widely used very often because files have small amount of redundant data.
2) Image steganography: This is used widely for hiding information in the cover image.
3) Audio/Video steganography

CRYPTOGRAPHY VS STEGANOGRAPHY

Cryptography is the science of encrypting data in such a way that one cannot understand the encrypted message, whereas in steganography the mere existence of data is concealed, such that even its presence cannot be noticed.

Using cryptography might raise some suspicion whereas in steganography the existence of secret message is invisible and thus not known.

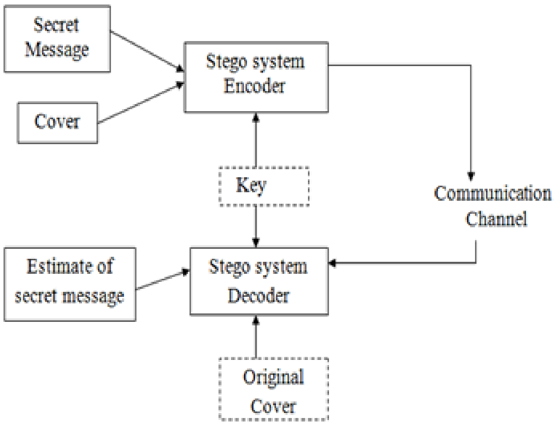


Fig1: Diagram of Steganography

We can think of steganography as an extension of cryptography, and it is commonly used under the circumstances where encryption is not allowed.

The basic principle of Steganography is carried out into two phases – 1. Sender Side Phase 2.Receiver Side Phase. In Sender Side Phase, Steganography Embedding Algorithm will takes three inputs - i) Secret Message ii.) Cover Image iii.)Stego-Key. After embedding data behind cover image embedding algorithm produce a new Stego image as output.

This newly generated Stego Image is transmitted to the designated Receiver over communication channel. In Receiver Side Phase, Steganography Extraction Algorithm will also takes two inputs – i.) Stego Image ii.)Stego-Key. After processing Stego image with the help of Stego-Key extraction algorithm will produce original secret message as output. This paper is organized into several following sections - Section – II describes image steganography in the field of data hiding. Section –III deals with the details of pixel mapping method. Section – IV&V explains the existing and proposed algorithm. Section – VI&VII describe result analysis conclusion.

Steganography is different from cryptography so both can be seen as complement to each other's. In cryptography plaintext/secret message is encoded into cipher form so that an attacker cannot easily decode cipher text into original secret message on the other hand Steganography is used to hide the existence of secret payload.

II. IMAGE STEGANOGRAPHY

As stated earlier, images are the most popular cover objects used for steganography.

In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

There are three stages performed in the image steganography. They are:

1. Image definition
2. Image Compression
3. Image and Transform domain

Encoding:

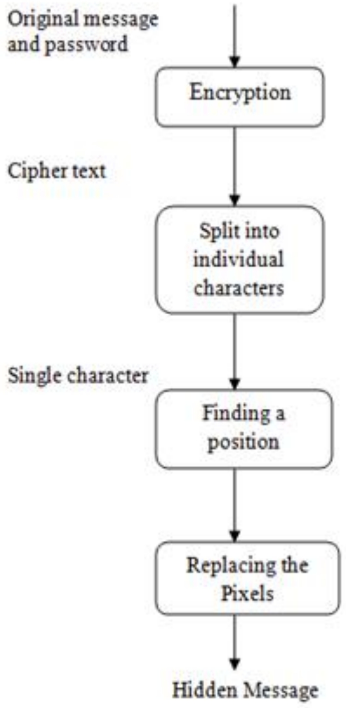


Figure 2: Flowchart of Encoding

Decoding:

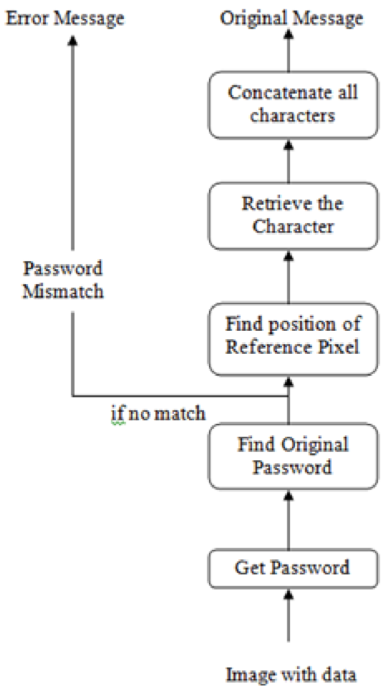


Figure 3: Flowchart of Decoding

Applications

Steganography is applicable to, but not limited to, the following areas.

1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system for digital content distribution
4) Media Database systems

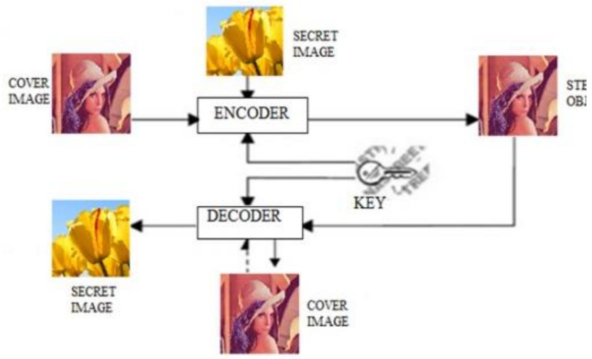
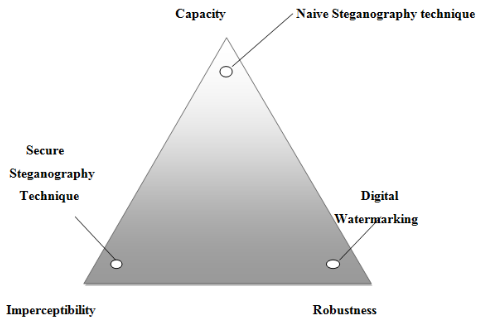
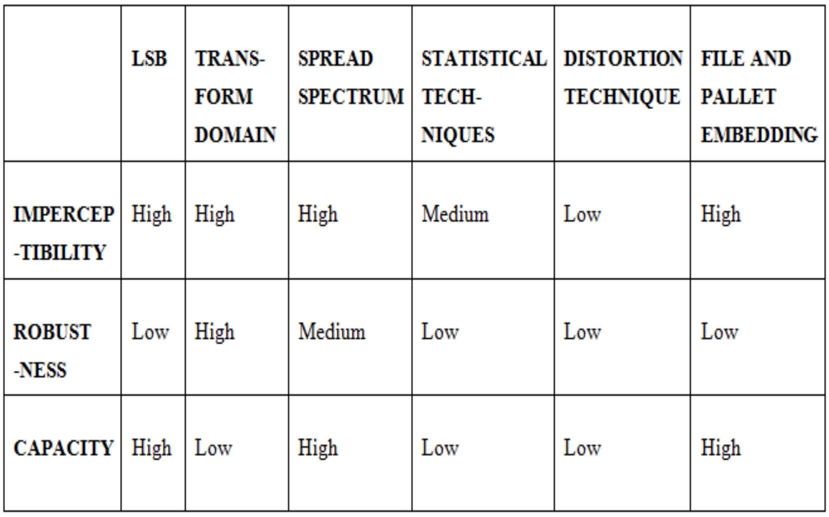


Figure 4: Block Diagram of Image Steganography

To hide the secret message in cover image the proper cover image should be selected. It is very important to hide the information in digital image using pixel mapping algorithm, because there is a chance for losing of information at the time of communication. Figure 4 shows how the secret image and cover image are embedded and retrieved using a key. At first, the cover image and secret image and encoded using a secret key then it becomes the stego object. Then using the same key as in the encoder side, we retrieve the data as we send. This process is analyzed by Histogram analysis. By doing histogram analysis, we are able to understand whether the information is embedded or not.

Comparison of Image Steganography Techniques





	LSB	TRANS-FORM DOMAIN	SPREAD SPECTRUM	STATISTICAL TECH-NIQUES	DISTORTION TECHNIQUE	FILE AND PALLET EMBEDDING
IMPERCEP-TIBILITY	High	High	High	Medium	Low	High
ROBUST-NESS	Low	High	Medium	Low	Low	Low
CAPACITY	High	Low	High	Low	Low	High

Table 1: Comparison of Image Steganography Techniques

III. PIXEL MAPPING

Pixel mapping is a function that maps (transforms)the colors of one (source) image to the colors of another (target) image. A color mapping may be referred to as the algorithm that results in the mapping function or the algorithm that transforms the image colors. Color mapping is also sometimes called color transfer or, when grey scale images are involved, brightness transfer function (BTF).

There are two types of color mapping algorithms: those that employ the statistics of the colors of two images, and those that rely on a given pixel correspondence between the images.

A common algorithm for computing the color mapping when the pixel correspondence is given is building the joint-histogram of the two images and finding the mapping by using dynamic programming based on the joint-histogram values.

When the pixel correspondence is not given and the image contents are different (due to different point of view), the statistics of the image corresponding regions can be used as an input to statistics-based algorithms, such as histogram matching. The corresponding regions can be found by detecting the corresponding features.

Pixel aspect ratio (often abbreviated PAR) is a mathematical ratio that describes how the width of a pixel in a digital image compares to the height of that pixel.

Most digital imaging systems display an image as a grid of tiny, square pixels. However, some imaging systems, especially those that must be compatible with standard-definition television motion pictures, display an image as a grid of rectangular pixels, in which the pixel width and height are different. Pixel Aspect Ratio describes this difference.

APPLICATION:

Color mapping can serve two different purposes: one is calibrating the colors of two cameras for further processing using two or more sample images; the second is adjusting the colors of two images for perceptual visual compatibility.

Color calibration is an important pre-processing task in computer vision applications. Many applications simultaneously process two or more images and, therefore, need their colors to be calibrated. Examples of such applications are: Image differencing, registration, object recognition, multi-camera tracking, co-segmentation and stereo reconstruction.

IV. EXISTING SYSTEM

The existing system on this paper has the following limitations

- Lesser data hiding
- 2D algorithm-limited features
- LSB algorithm
- Gray Scale image etc

There are many versions of spatial steganography. All those methods directly change some bits in the image pixel values in hiding data. Least significance bit-based steganography is one of the simplest techniques that hide a secret message in the LSBs of pixel values without introducing many observable distortions. To our human eye, changes in the value of the LSB are unnoticeable. Thus, LSB can be used as an ideal position for hiding information. This does not involve any perceptual change in the cover object. Embedding of message bits can be done either in sequence or at random. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images. It is being predicted that the proposed method will able to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method.

V. PROPOSED SYSTEM

In this paper several conventional methods have been examined to assess their effectiveness in pixel locating identification. Despite the delicate adjustment of many parameters in the use of these methods, the results were still unsatisfactory. Edges extracted from nontrivial images are often hampered by fragmentation, meaning that the edge curves are not connected, edge segments are melted, or false edges that do not correspond to significant phenomena in the image are shown. It is therefore desirable to develop a dedicated pixel location method for image steganography method. Accordingly, a new computing algorithm is proposed in this paper to process a pixel editing and to identify the edges of images. Hence it will be useful to hide the secret data in the image.

PIXEL SELECTION METHOD

In our proposed technique we are consecutively selecting pixels to embed message bits into chosen pixel. We can also employ an arbitrary function 2r+ 5 % width to choose pixels in random way where r represents row of image. By using arbitrary locations we can develop the protection of clandestine communication. But sometimes, it may degrade the embedding capacity.

FEATURES OF PROPOSED SYSTEM

The following are some of the features of the proposed system:
This algorithm provides a useful addition to Secret image processing.

- Analysis in Pixel mapping scheme.
- The work presented was aimed for the processing of pixel.
- Further work is required to evaluate the performance of the algorithm in real-life steganography scenarios.

VI. RESULTS ANALYSIS

The performance characteristics of the image steganography using pixel mapping are simulated. The various performances namely cover image, secret image, 4-bit image to hide, stego image and also histogram analysis of cover image and stego image are analyzed for the proposed algorithm. This is original image (without hidden information). The file format of this image is BMP (Bitmap Pixels). The extension of this file is .bmp. To embed the text into the original image , get the information from the user in the format file name with extension (.bmp).Usually the information is embedded into the image is in the format of image. Its file extension must be .bmp. The secret information is pixel mapped, so the secret image is changed to 4-Bit Image. Then the image is hidden on the original image. After embedding some information into the original image we get the stego images (with hidden information).Since it is color image the large number of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded. The other benefits are that a much larger amount of hidden data can be encoded into a 24-bit digital image. After embedding some information into the original image, the stego image looks very much similar to the original image. Since the color image consists of 24 pixels, there is no fading occurred in the stego image.

For the human vision, there is no difference between original image and stego image. Hence, we are going to check the histograms of both original and stego image. X- axis represents the resolution value of the image and Y- axis represents the intensity of the image. Sudden rise or peak in the histogram denotes that some information has been hidden in the particular pixels.

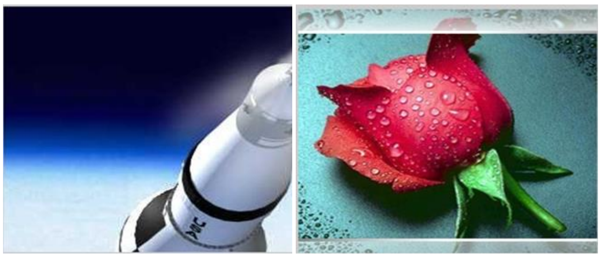


Fig 5: Cover Image (left) and Stego Image (right)

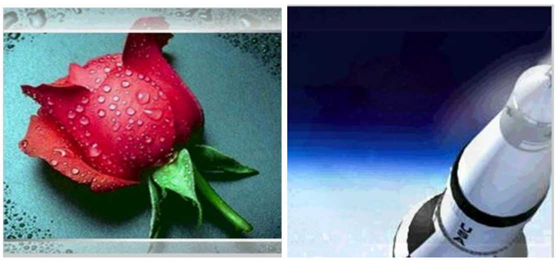


Fig 6: 4-bit image to hide(left) and Stego image(right)

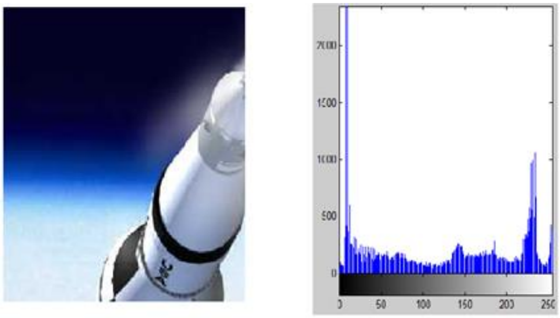


Fig 7: Histogram analysis for cover Image

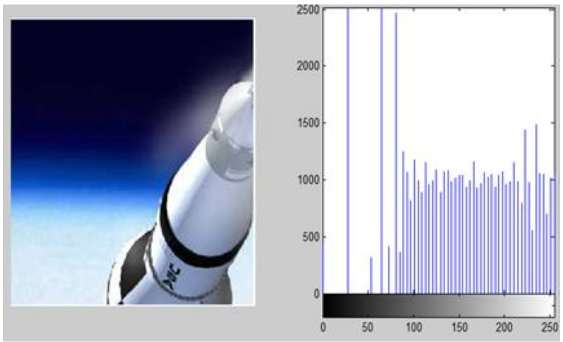


Fig 8: Histogram analysis for stego Object

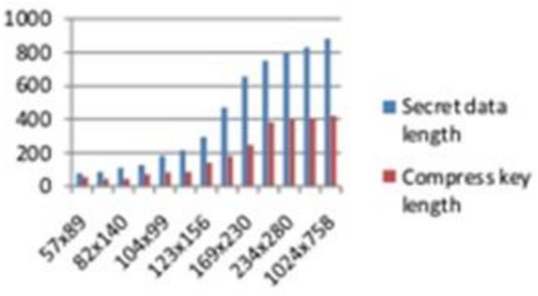


Fig 9: Relationship between secret data length and compress key length

VII. CONCLUSION

Data hiding is a challenging and most important task in the field of information security. In this paper we have proposed a pixel mapping algorithm which is able to hide secret information in the colored RGB image having 24-bit format. By using this algorithm, we are capable of hiding the more data in which the intruder does not know what information is transferred. For the security purpose only we are going for steganography.

REFERENCES

[1] Fridrich Jessica M. Goljan; D. Soukal (2004). "Searching for the Stego Key" (PDF).Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 5306: 70–82. Retrieved 23 January 2014.

[2] Prashanthi.G,SandhyaRani.K, Deepthi.S “LSB and MSB Based steganography for Embedded Modified DES Encrypted Text”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3,Issue 8,August 2013,pp.788-799.

[3] DeepeshRawat, VijayaBhandari,“Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method”, International Journal of Computer Applications, Vol.67, No.1, April 2013,pp.22-25.

[4] Prince Kumar Panjabi and Parvinder Singh, “ An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach”, International Journal of Computer Applications (0975 – 8887) Volume 74– No.10, July 2013.

[5] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” IEEE Trans. Inf. Forensics Secure., vol. 1,no. 1, pp. 111–119, Mar. 2006.

[6] Souvik Bhattacharyya and Gautama Sanyal, “Study and analysis of quality of service in different image based Steganography using PMM” International journal of applied information system – foundation of computer science, New York, USA 2012.

[7] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[8] Clair, Bryan. "Steganography: How to Send a Secret Message", www.strangehorizons.com / 2001 / 20011008 /steganography.shtmI8Nov.2001.

[9] M.Sivaram B.DurgaDevi J.Anne Steffi, “Steganography of two lsb bits”, International Journal of Communications and Engineering, Vol.1– No.1, Issue: 01, March 2012.

[10] WaiWaiZin,”Message Embedding In PNG File Using LSB Steganographic Technique”, International Journal of Science and Research (IJSR) Vol. 2 Issue 1, January 2013, pp. 227-230.

[11] S. Rubab and M. Younus, “Improved Image Steganography Technique for Colored Images using Wavelet Transform”, International Journal of Computer Applications, Volume 39– No.14, pp. 29-32, 2012.

[12] Ravi Kumar, KavitaChoudhary, NishantDubey, “An Introduction of Image Steganographic Techniques and Comparison”, International Journal of Electronics and Computer Science Engineering.

[13] Mamta Juneja, Parvinder S. Sandhu, and EktaWalia,”Application of LSB Based Steganographic Technique for 8-bit Color Images”, World Academy of Science, Engineering and Technology,2009.

[14] K. Hemp stalk, “Hiding behind corners: using edges in images for better steganography”, Computing Women Congress Conference, Hamilton, New Zealand, 2006.

[15] S. Roy and R. Parekh, “A Secure Keyless Image Steganography Approach for Lossless RGB Images.” Proceedings of International Conference on Communication, Computing & Security, ACM Publications, 573-576, 2011.