Image Steganography and Steganalysis Using Pixel Mapping Method

Mrs.K.Rajasri,M.Tech.,M.I.S.T.E.,
Senior Assistant Professor,

Christ College of Engineering and Technology,

Puducherry.

Mrs.D.Gayathri,M.Tech.,M.I.S.T.E.,
Senior Assistant Professor,

Saveetha Engineering College,

Chennai.

Ms.T.Indhumathi,M.Tech.,
Student,

Christ College of Engineering and Technology,
Puducherry.

Abstract

Steganography is a method that involves embedding a communication in a suitable carrier for example an image or an audio file. The carrier can then be send to a recipient with no one else knowing that it contains a concealed communication. The aim of this work was to investigate the various steganography methods and how they are employed for clandestine communication .LSB is a very fine recognized means in this field. In binary images we are very much limited in the span as there are only 4 bits or 8 bits to be a symbol of a pixel which leads us to the restriction of using most popular LSB methods .But in coloured images there are in general up to 24 bits images with three diverse RGB channels, if using RGB colour space .So, we can investigate a lot many new methods which can operate or use various channels of coloured images in regular or arbitrary sample to conceal the information. Using this idea we have explored the different active methods of data hiding in coloured images and taken an intersection between the arbitrary pixel manipulations, LSB method and Bit-Plane Complexity Segmentation to propose our work which uses random channel and a pixel mapping method to reveal the occurrence of data in one or two other channels. We have proved that this effort shows an attractive outcome as compared to the other present algorithms on the various parameters like security, imperceptibility capacity and robustness. At the last part the new steganography procedure is also compared with the available techniques.

1. Introduction

Techniques for information hiding have turn out to be more and more refined and well-known. [4, 5] The information is made puzzling and this is accomplished with Cryptography and Steganography.

1.1 Steganography vs. cryptography

In everyday time early from the magazines, to the normal media outlets, scientific journals, political campaigns, courtrooms and the photo hoaxes lands in our email inboxes, occurrence of digital techniques is considered to be ordinary and they are employed with increased rate. Data Hiding is one of the difficult issues in the field of Network Security. [11]

In cryptography, the information is able to be seen but not in any meaningful appearance. Only by knowing the cryptographic algorithm, the hidden data can be deciphered**.** In cryptography everyone knows that there is hidden information present. But, only the right algorithm can disclose. i.e. in cryptography a message can be easily seen and recognized as cryptic message but only the one who has information as how the data is encrypted will come to know how to decrypt it.

Cryptography was formed as a method for securing the confidentiality of message. Many different methods have been developed to encrypt and decrypt data in order to keep the message clandestine. Unfortunately, it is sometimes not sufficient to stay the contents of a message secret. So, it is necessary to keep the survival of the message secret.

Unlike cryptography, Steganography is used to conceal the existence of clandestine communication by embedding the communication behind any envelop article like image, text, audio, video files. Network steganography shelters a broad spectrum of techniques.

Digital watermarking is the method of embedding information into digital multimedia content such that the information can later on be extracted or detected for a diversity of purposes together with copy avoidance and organize. Digital watermarking has become a dynamic and significant region of learning and growth. The commercialization of watermarking techniques is being deemed necessary to assist some of the challenges faced by the brisk creation of digital content. The key distinction stuck between information hiding and watermarking is the lack of an active opponent. In watermarking applications like copyright safeguard and confirmation, there is an active opponent that would try to eliminate, cancel or falsify watermarks. In information hiding there is no such lively enemy as there is no value related with the operation of removing the information hidden in the content. Nevertheless, information hiding techniques necessitate being stout against accidental distortions. Watermark insertion at the source side include the generation of the watermark signal *W* and embed W in the original image *I* to get a watermarked image *I'*. The other side is to extract the watermark *W*, and give the confidence measure for the detected image. Figure 1 shows the generic watermark embedding at the source side. We have the watermarked image $I' = f1\ (I, W, K)$, where *K* denotes the key.

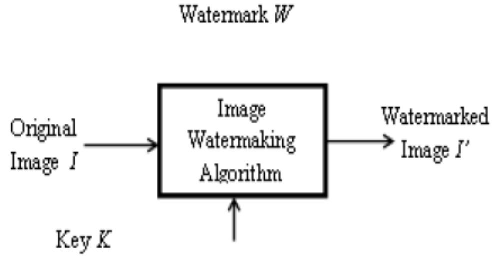

Figure 1. Generic Watermark Insertion

Unlike information hiding and digital watermarking, the main objective of steganography is to converse strongly in a totally untraceable way. JPEG images are most widely used in watermarking and steganography methods.

Images are the most common carrier medium. They are used for steganography in the following approach. The message may firstly be encrypted. The sender embeds the clandestine communication to be sent into a graphic file. This results in the creation of what is called a stego-image. Additional clandestine data may be essential in the hiding process e.g. a stego key. The stego-image is then transmitted to the receiver. The receiver takes the communication from the carrier image. The message can only be extracted if there is a shared secret flanked by the sender and the recipient. This might be the algorithm for removal or an unusual consideration such as a key. One of the commonly used techniques is the LSB where the least significant bit of each pixel is replaced by bits of the secret till secret message finishes.

Steganography refers to the method of hiding secret mail into media such as text, audio, image and video without any doubt. [12] It can be employed for the advantage of the mankind to serve us as well as by terrorists and criminals intended for wicked purposes. In the history, diverse steganographic techniques with properties of imperceptibility, undetectability, robustness and ability have been projected.

To hide the information within any media engage very important features like a cover medium or file which is necessary for hiding data , a secret data that required to be hidden and a key or code word that may be used by sender and receiver for encryption and decryption.

Steganography has its Greek origin and means secrete writing. Here, 'stega' means covered from Greek word steganos and 'nography' means writing from Greek word graphia.

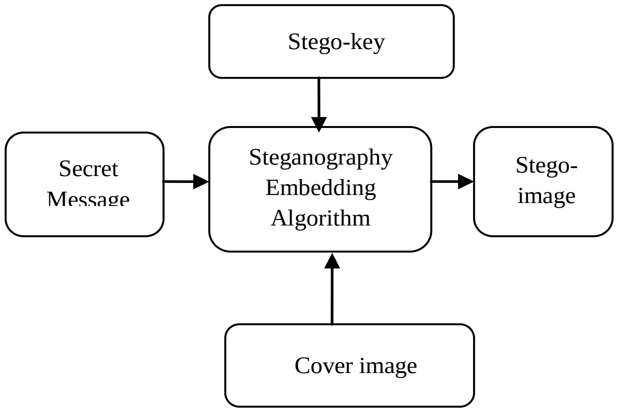

Figure 2. Generic Form of Steganography at Sender Side

The method of steganography starts by identifying the cover image and the information which is to be concealed. Steganography is an ancient art but digital expertise gives it novel way so that can be hide information in digital images and signals also. The goal of steganography is to insert a message within an innocuous looking cover medium so that casual inspection of the resulting medium will not disclose the existence of the message.

For example, with plain text as a cover medium, a German spy, during World War I, sent the following message:

Apparently neutral's protest is thoroughly discounted and ignored. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

This upon casual inspection seems fairly safe. When the second letter of each word is extracted, however, this text is seen to be a carrier for the following message:

Pershing sails from NY June 1.

With the advent of the Internet and the broad propagation of large amounts of digital media, digital images have become a popular cover medium for steganography tools. In addition to being nearly ubiquitous on most web pages, digital images are well suited as a cover medium. An uncompressed colour image of size 640 X 480, for example, can hide approximately 100 000 characters of text.

1.2 Steganalysis

Newer and more stylish steganographic methods for embedding secret communication will require more dominant steganalysis methods for recognition. Steganalysis is the art of attacking steganography in a conflict that never ends.

Steganalysis is the ability and discipline of uncovering of the existence of steganography. Steganalysis is a method of detecting clandestine communication hidden using steganography. The goal of steganalysis is to gather enough proof about the existence of embedded message and to break the security of its carrier. Thus break the security provided by steganography. Both steganography and steganalysis have received a lot of notice from law enforcement and media. The battle stuck between steganography and steganalysis is never comes into conclusion.

The ultimate goal of steganalysis is to decide if an image contains an embedded message. As this field has developed, determining the length of the message and the actual contents of the message are also becoming active areas of research.

There are two approaches to the crisis of steganalysis. One is to come up with a steganalysis means exact for a particular steganographic algorithm. The other is just beginning techniques which are independent of the steganographic algorithm to be analyzed. Each of the two methods has its own merits and demerits.

The importance of steganalytic techniques that can reliably notice the existence of concealed information in images is increasing. Steganalysis is classified into: Statistical Steganalysis and Signature Steganalysis. When secret data hides in an image then the statistics of an image changed. Due to add of this secret information in the image, its pixel values alter. This alter in statistic of the image is used during analysis to notice the secret data. So, current steganalysis methods fall broadly into one of two categories: embedding specific or universal (e.g., [1]). While universal steganalysis attempts to detect the existence of an embedded message independent of the embedding algorithm and, ideally, the image format, embedding specific approaches to steganalysis take advantage of particular algorithmic details of the embedding algorithm. Blind steganalysis based on classifying quality vectors imitative from images is becoming more and more powerful. [4] Given the ever growing number of steganography tools, universal approaches are clearly necessary in order to carry out any type of generic, large-scale steganalysis.

Universal statistical steganalysis consist of those statistical steganalysis techniques that are not employed for a particular steganography hiding method. The main idea behind these techniques is to find out some suitable statistical quantities having 'distinguishing' capabilities. SVM, Neural network, clustering algorithms and other techniques are then used to create the discovery model from the trial data of these tools and techniques.

A steganalysis procedure specific to an embedding process would give very excellent results when tested only on that embedding process, and might be unsuccessful on all other steganographic algorithms.

JPEG (Joint Photographic Experts Group) is a lossy compression format. It means that once we save the image, any details that are lost cannot be recovered. In this inspection, lossy image compression schemes such as JPEG might be considered a forensic analyst's worst enemy. It is ironic, so, that the unique properties of lossy compression can be exploited for forensic analysis. Now we explain three forensic techniques that detect tampering in compressed images, each of which explicitly leverages details of the JPEG lossy compression scheme.

When an image is cropped and recompressed, a new set of blocking artifacts may be introduced that do not essentially align with the original margins. Within- and across-block pixel value differences are computed from 4-pixel neighborhoods that are spatially offset from each other by a fixed quantity, where one neighborhood lies entirely within a JPEG block and the other borders or overlaps a JPEG block. A histogram of these differences is computed from all 8 × 8 non overlapping image blocks. An 8 × 8 ―blocking artifact matrix (BAM) is computed as the average difference between these histograms. For uncompressed images, this matrix is random, while for a compressed image, this matrix has a specific pattern. When an image is cropped and recompressed, this pattern is disrupted. Supervised pattern classification is used to discriminate between authentic and inauthentic BAMs.

In our proposed work we are going to employ the pixel mapping method. This can be effectively used to hide the secret information behind the grey scale images and coloured images.

2. Existing Scheme

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.

The image is decomposed to a set of binary images according to the bit-plane complexity segmentation, which divides bit-plane into successive and non-overlapping blocks. Each block is further checked whether it is noise-like or not, and noise-like blocks are suitable for embedding information.

JPEG is based on DCT in lossy compression and it is the most common format of images produced by digital cameras, scanners and other photographic capture devices. In JPEG compression, successive sub-image blocks of size of 8X8 on applying DCT produces 64 DCT coefficients, and data can be inserted in these coefficients' insignificant bits. However, changing any single coefficient would influence the entire 64 block pixels. No visible alteration can be seen in the stego-image as the changes due to insertion data are in frequency domain. JSteg embeds secret message into a cover image by consecutively replacing the LSBs of non-zero DCT coefficients with message bits. Then PSNR value can be calculated using PSNR = 10 log $_{10}$ MAX^2/MSE (db).

LSB Steganography can be classified by two methods LSB substitute and LSB matching. The Now LSB embedding causes the occurrence of individual essentials of a Pairs of Values to flatten out with respect to one another. So for example if an image has 100 pixels that have a value 2 and 200 pixels that have a value 3, then after LSB embedding of the entire LSB plane the accepted frequencies of 2 and 3 are 150 and 150 respectively. This of course is when the whole LSB plane is customized. Though, as long as the embedded message is great adequate, there will be a statistically visible flattening of Pairs of Value distributions and this fact is demoralized by their steganalysis method. LSB embedding can only be constantly detected when the message span becomes equivalent with the quantity of pixels in the image. In the case where information assignment is recognized, shorter communication can be detected. Existence of hidden message can be found visually, and JSteg can be easily detected by Chi-Square - test.

The ensemble

The ensemble classifier consists of countless base learners, separately trained on a set of cover and stego images. [8] The initial phase consists of retrieving the necessary information required for decoding from the corner pixels. In the first step we need to retrieve two important parameters from the encrypted image as secret message size and order of the stego images. After selecting the stego image, steganalyst should enter the key for decoding.

The primary supply of difference in the encoders is the option of quantization table. Visual examination or simple information from stego-images can yield sufficient tell-tale proof to differentiate between stego and cover-images.

Then we intend decoding the original message from the stego image and concatenate them in order to obtain the secret message. We first, apply the sampling algorithms to obtain the samples used for encoding. Then we proceed as below:
Step 1: From the samples obtained, we get the values of the second level encrypted message E. We evaluate the message as:
e0 = E0
ei = Ei XNOR ei-1, Where E is the second level encrypted message and e is the first level encrypted message.

Step 2: Then we decrypt the message e as, Loop from O to the size of the message
e -> O to n(e).
if I is a factor of n(e) then,
Oi = ei + dec – 3 lsb
else
Oi= ei - dec – 3 lsb

The main crisis of this method is that, hiding the information in the channels is done in a logical way. So, being able to find out the information in the first few pixels will make the detection of the technique easy. StegoPRNG is also a different technique that uses the RGB images. However in this method, a pseudo random number generator is used to choose some pixels of the cover image. The length restraint, on the other hand, turns out to be the central restriction of this technique. There are various LSB detectors like RS, SPA , DIH etc. are hard to detect that in active way due to two restrictions. Initially, high detection fault at low embedding rate. Secondly, this method is not capable to notice the precise embedding position.

3. Proposed Scheme

Initial step is to take the secret message, path of cover image and path of output image from the user. Then read the cover image in a three dimensional array. Here, we propose the pixel mapping method for the purpose of hiding the information in digital media. Pixel mapping method uses the idea of pixel intensity and number of one's in pixel to map information. This approach produces improved embedding ability and PSNR Value over PVD and GLM methods. If we use this PMM method with BPCS, this approach produces better image quality over the use of PMM method alone. If the 2 LSBs of reflecting outlet is 00 then this pixel does not contain any clandestine information and go to step of sampling.

3.1 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.

3.2 Sampling

Sampling is intricately connected with booming steganography and plays a vital responsibility in this procedure. The samples are selected based on the input cover object, secret massage and the stego key. Further, a striking characteristic of the sampling task is that the sample count decreases exponentially as we move inwards from the periphery to the Centre of the picture. This is based on the plan that the interior of the picture is usually more carefully noticed and focused on by the human eye, and peripheral parts generally attract slighter detailed and dedicated notice. The sampling is strengthened keeping in mind the visible changes in the histogram, thereby repulsing steganalysis cleverly. Further, the task ensures that roughly equal number of pixel samples have been selected from all four quadrants, to avoid clustering of samples from a single one.

To eliminate the restraint of a predetermined size secret message, we intent to put forward an automatic adjustment algorithm. This section is mainly concerned with ensuring that input secret message size to be embedded bears a fairly sensible ratio to the cover image size for which the deformation is insignificant. The dynamic ratio value is defined depending on the dynamics of the image and the concentration of the colour component values across the cross sections of the image. Based on the above concept, our algorithm warns against suspicion. This suggests the use of an extra cover image or the copy of the same cover image, which can be generated repeatedly. On contract we divide the secret information in the best-proportion and then re-sample it. This method of splitting and re-sampling is a recursive procedure and terminates once an optimally allowed ratio is reached. We store the necessary values mandatory for decoding in the four corners of a picture.

3.3 Resampling

The estimated probability is then employed to decide if a part of the image has been resampled. A common form of photographic manipulation is the photomontage. Photomontage is a paste-up created by sticking together photographic images, possibly followed by post- processing. It uses digital splicing of two or more images into a single composite. When performed cautiously, the edge between the spliced regions can be visually unnoticeable.

This improved approach can also be employed to embed 8 bits data by extending mapping rules. There are many key merits for this approach. They are unauthorized individual cannot retrieve data without the knowledge of mapping rules. It can provide better safety by mapping data into arbitrarily selected pixels. It has low computational overhead over other Steganography approaches since it does not need change of images into frequency domain. Finally, the ultimate aim is achieved i.e. only sender and receiver know about the information.

4. Conclusion

Thus a new robust method for steganalysis using pixel mapping method is proposed. This method uses the concept of pixel intensity and no of one's in pixel to map data. This is more efficient than the previous methods. It has low computational overhead and provides better security. This is an efficient approach to plot secret communication into gray scale images to provide improved image quality and information embedding capacity.

5. References

[1] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," presented at the 6th International Workshop on Information Hiding, Toronto, ON, Canada, 2004.

[2] R.Fisher, S.Perkins, Awalker and Walfort "Fourier Transform".

[3] Johnson Neil F., Zoran Duric, Sushil Jajodia, "Information Hiding, and Watermarking - Attacks & Countermeasures", Kluwer 2001.

[4] H. Farid and S. Lyu, "Detecting hidden messages using higher-order statistics and support vector machines," in 5th Information Workshop Information Hiding, 2002, vol. 2578, pp. 340–354.

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

[6] T. Pevny and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis," in Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505, pp. 31–314, 2007.

[7] Y. Shi, C. Chen, and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," in 8th Int. Workshop Information Hiding, vol. 4437, pp. 249–264, 2006.

[8] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifier for steganalysis of digital media," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 432–444, Apr. 2012.

[9] P. Sallee, "Model-based methods for steganography and steganalysis," Int. J. Image Graph., vol. 5, no. 1, pp. 167–190, 2005.

[10] Der-Chyuan Lou et. al. "Active steganalysis for histogram-shifting based reversible data hiding", Elsevier, Optics Communications 285 , 2012, pp.2510–2518.

[11] 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.

[12] Yambem Jina Chanu, Kh. Manglem Singh, Themrichon Tuithung, "Image Steganography and Steganalysis: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012.