International Research Journal in Global Engineering and Sciences. (IRJGES)
Vol. 1, No. 1, May, 2016 | ISSN : 2456-172X

Exploring knowledge on Image Retrieval with Data hiding Technique

[1]Dr.E.D.Kanmani Ruby, [2]Dr. M. Thangamani,
[1]Professor, Department of ECE, Kongu Engineering College, Perundurai -638 052, India
[2]Assistant Professor, Kongu Engineering College, Perundurai -638052, India

Abstract: Nowadays, security for any data is of major concern. Steganography is the practice of concealing messages or information within other non-secret text or data. Reversible data hiding .is used to embed secret message into a cover image by slightly modifying its pixel values. Embedded message and the cover image are completely recovered from the marked content. It supports information hiding with the lossless compressibility of natural images. In this article explore the image retrieval information along with data hiding methods.

Keywords: Steganography, Embedded message

1. INTRODUCTION

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word steganography combines the Ancient Greek word steganos, meaning "covered, concealed, or protected", and graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic.

The hidden messages will appear to be something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle. Steganography has been widely used, including in recent historical times and the present day. Known examples include: Hidden messages within wax tablets in ancient Greece, people wrote messages on the wood, and then covered it with wax upon which an innocent covering message was written. Hidden messages on messenger's body also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.

Modern steganography entered the world in 1985 with the advent of the personal computers being applied to classical steganography problems. Development following that was very slow, but has since taken off, going by the large number of steganography software available: Concealing messages within the lowest bits of noisy images or sound files. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data. Chaffing and winnowing. Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack. Digital steganography output may be in the form of printed documents. A message, the plaintext, may be first encrypted by traditional means, producing a ciphertext. Then, an innocuous cover text is modified in some way so as to contain the cipher text, resulting in the stego text.

Unicode steganography uses lookalike characters of the usual ASCII set to look normal, while really carrying extra bits of information. If the text is displayed correctly, there should be no visual difference from ordinary text. Some systems, however, may display the fonts differently, and the extra information would be easily spotted. Hidden characters and redundant use of markup can add embedded within a body of text to hide information that wouldn't be visually apparent when displayed, but can be discovered by examining the document source. HTML pages can contain code for extra blank spaces and tabs at the end of lines, as well as different colors, fonts and sizes, which will not be visible when displayed.

In general, terminology analogous to more conventional radio and communications technology is used; a brief description of some terms which show up in software specifically and are easily confused is appropriate. These are most relevant to digital steganographic systems. The payload is the data to be covertly communicated. The carrier is the signal, stream, or data file into which the payload is hidden; which differs from the "channel". The resulting signal, stream, or data file which has the payload encoded into it is sometimes referred to as the package, stego file, or covert message. The percentage of bytes, samples, or other signal elements which are modified to encode the payload is referred to as the encoding density and is typically expressed as a number between 0 and 1.

Detection of physical steganography requires careful physical examination, including the use of magnification, developer chemicals and ultraviolet light. It is a time-consuming process with obvious resource implications, even in countries where large numbers of people are employed to spy on their fellow nationals.

2. RELATED WORK

Wien Hong et al. [1], the reference pixel-based methods are extended by applying a variety of embedding schemes. Here, the concept of dual binary tree has been applied for the embedment of data which helps in increasing the payload to a greater extent. The predictor has been used to obtain the predictor errors and an energy estimator has been used to calculate the energy of each prediction error. Thus, the embedding efficiency has been greatly increased.

In the histogram-shifting method, initially, each local image region is projected to a one-dimensional space to obtain a scalar sequence which is followed by the generation of one-dimensional histogram. Secondly, the data are embedded into the cover image by modifying the histogram. A local image region has been considered and then it is projected to a two dimensional space to get a sequence which consists of difference-pairs. Then, a two-dimensional difference-histogram is generated by counting the difference-pairs [2]. Here more number of pixels has been used for carrying data with the significant reduction in the number of shifted pixels and significant improvement in the embedding mechanism.

Video Steganography falls under two categories: The one being the embedment of the secret message in the pixels of the video frames directly [3]. The other one hides the secret message into the compressed domain of the videos by modifying the variable length codes, prediction modes and the motion vectors. For video Steganography in spatial domain, in order to guarantee the successful recovery of hidden message after potential distortion due to lossy compression or channel noise, it usually encodes the message with error correcting code and embeds them into multiple locations, which resists the video compression to some degree but limits the embedding capacity. The other category is specially designed for compressed video. It directly modifies the coefficients in the compressed domain, thus it integrates Steganography directly into the compression scheme but is fragile to any distortion and the embedding capacity is also limited because there are fewer coefficients which can be modified to carry the secret message.

In the paper [4], a spatial domain-based binary image steganographic scheme is proposed. The scheme minimizes a novel flipping distortion measurement that takes into account both the Human Visual System and statistics. This measurement employs the weighted sum of complement, rotation and mirroring-invariant local texture pattern (crmiLTP) changes to measure the flip. The weight value corresponding to each crmiLTP is set according to the sensitivity of the pattern to the embedding distortion. The proposed steganographic scheme presents a significant performance compared with state-of-the art works.

The stego image with a low embedding ratio is usually detected more difficultly; the steganalysis of the stego image with a low embedding ratio has been one of the important and difficult issues of steganalysis [5]. Although the structural steganalysis can estimate the low embedding ratio with less error than others, the existing structural steganalysis methods for Multiple Least Significant Bits (MLSB) steganography only utilize the correlation between two adjacent samples. For Least Significant Bit (LSB) replacement, the structural steganalysis methods utilizing the correlation among more than two adjacent pixels can usually estimate the low embedding ratio with higher precision. Intuitively, one should also be able to improve the estimation accuracy for the low embedding ratio of MLSB steganography by utilizing the correlation among more adjacent pixels. HS-based Reversible Data Hiding (RDH) is implemented by modifying host image's histogram of a certain dimension. It has two major advantages. On one hand, the maximum modification to pixel values can be controlled and thus the embedding distortion can be well limited [6]. On the other hand, the location map used to record underflow/overflow locations is usually small in size especially for low ER case. As pointed out by Sachnev et al., RDH algorithm with smaller, or in some cases, no location maps, are very desirable. Therefore, HS is a good choice among existing approaches of RDH.

Data hiding is an art of data concealment in which the presence of embedded messages cannot be detected. Digital images are often used for carrying data in many data hiding techniques because they are often delivered over the Internet. If a digital image is served as a message carrier, the image for carrying data is called a cover image, and the image that carried data is called a stego image. During data embedding, distortion of images occurs since the pixel values in the cover image will be inevitably changed. If the embedding algorithm has no capability to recover the distorted pixels back to their original ones, then this type of embedding is termed lossy embedding. On the other hand, if the stego image can be recovered to its original state after extracting the secret data, the corresponding embedding technique is termed lossless or Reversible Data Hiding. Reversible data hiding techniques can be performed both in spatial domain and in compressed domain [7]. For spatial domain embedding, pixel values in the cover image are modified so that data can be embedded into pixels. Reversible data hiding of this domain often achieves larger payload because images in spatial domain provides rich redundancies, which are suitable for data embedding. For compressed domain embedding, data are embedded by modifying the compressed codes. For example, the index table of VQ-compressed codes can be modified for carrying data. Embedding data in compressed domain sometimes is preferred because compressed codes are beneficial for saving the storage space.

However, these methods often suffer from lower payload and higher computational cost because they are performed in compressed domain, and redundancies in this domain are often smaller than those in the spatial domain.

Another reversible data hiding scheme based on modification of prediction errors was proposed by Tsai et al. in 2009. They selected a set of basic pixels as the predicted value of their neighbors and embed data bits into the histogram of prediction errors. In Tsai et al.'s method, pixel values are modified one grayscale at most to produce a high quality stego image; therefore, their method is suitable for applications requiring very low distortion such as medical imaging. However, Tsai et al.'s method does not fully exploit the correlation of neighboring pixels, leading to a less accuracy prediction results and subsequently reducing the amount of payload. Besides, their method does not consider the pixel activities in image blocks. Both smooth and complex blocks are processed using the same algorithm in the embedding phase, resulting in a considerable amount of image degradation. Although a high quality stego image can also be obtained in Thodi and Rodríguez, Hu et al., Sachnev et al. by limiting the changes of pixel values at most by one, their embedding algorithms are designed for general purpose and might not be optimized for applications requiring high quality image. In the system modified Tsai et al.'s work by introducing a basic pixel set consisting of five basic pixels. In the proposed method, the prediction accuracy can be significantly increased, and a local variance can be obtained to control the image quality. Therefore, a significant improvement over Tsai et al.'s method can be achieved.

Reversible image watermarking, which enables recovering both the original image and the watermark from the watermarked content, has aroused considerable interest recently. Many valuable reversible watermarking algorithms have been presented in the literature. Tian introduced a difference expansion (DE) based method, in which the difference of two adjacent pixels is expanded to carry one data bit [8]. This method usually provides high capacity while keeping the distortion low.

3. CONCLUSION & FUTURE WORK

This paper pictured review of the work already done in image retrieval with data hiding. There are many techniques available for data hiding in image. Reversible Data hiding is a technique which is recently used for the same. Histogram Equalization, Histogram shifting are the techniques applied for image analysis. Image histograms are highly useful for analyzing the image qualities and are highly beneficial for the purpose of data hiding. Hence, Multiple Histogram Modification (MHM) scheme to be employed for the data hiding process. The system can be enhanced to improve the embedding capacity with optimized predictor selection approach in future.

REFERENCES

[1] Wien Hong, Adaptive reversible data hiding method based on error energy control and histogram shifting, Elsevier, Optics Communications, Vol. 285, Issue 2, Pp. 101-108, 2012.

[2] Xiaolong Li, Weiming Zhang, XinluGui, and Bin Yang, A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification, IEEE Transactions on Information forensics and Security, Vol. 8, No. 7, Pp.1091-1100, July 2013.

[3]Keren Wang, Hong Zhao and Hongxia Wang, Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value, IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, Pp. 741-751, May 2014.

[4] BingwenFeng, Wei Lu, and Wei Sun, Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 2, Pp. 243-255, February 2015.

[5]Chunfang Yang, Fenlin Liu, XiangyangLuo, and Ying Zeng, Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, Pp. 216-228, January 2013.

[6] Xiaolong Li, Bin Li, Bin Yang, and Tieyong Zeng, General Framework to Histogram-Shifting-Based Reversible Data Hiding, IEEE Transactions on Image Processing, Vol. 22, No. 6, Pp. 2181- 2191, June 2013.

[7].W. Hong and T. S. Chen, “A Local Variance-Controlled Reversible Data Hiding Method Using Prediction And Histogram-Shifting,” J. Syst. Software, vol. 83, no. 12, pp. 2653–2663, Dec. 2010.

[8] Xiang Wang, Xiaolong Li, Bin Yang, and ZongmingGuo, Member, IEEE, Efficient Generalized Integer Transform for Reversible Watermarking, IEEE Signal Processing Letters, Vol. 17, No. 6, Pp. 567-570, June 2010.