International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

A Survey on Various Data Hiding Techniques

Remya Jose
Department Of Computer Science And Engineering
Amal Jyothi College Of Engineering
Kanjirappally , Kottayam, India

***Abstract*—Data is very essential in information system, so protecting the data from hackers is very important.Data should be secure while transferring the data from one location to another. Inorder to keep the transmitted information away from unauthorized users, a variety of techniques have been proposed, data hiding is one of the protective techniques in data security. Data hiding is a method used to embed secret data into a cover image. In this paper , we present an overview of recent research efforts in data hiding and its efficiency. We then evaluate the approaches based on important performance criteria. Some conclusions are developed regarding the suitability of particular design choices under various conditions.**

***Keywords*— Data hiding, Data embedding Capacity, Steganography , Secret Information.**

I. INTRODUCTION

The Internet provides great convenience to the transmission of a large amount of data over networks. These datas are open but insecure , exposing many private and secret data to dangerous situations. Today, it is important to ensure that information transmitted over the internet remains safe and secure. Since the inception of the internet, the security and the confidentiality of the sensitive information have been of utmost importance and of top priority.

A variety of techniques have been proposed to keep the unauthorized user away from the transmission information .Data hiding is one of the protective techniques in data security. Data hiding is a method which allows to embed secret data into a cover image, which can be performed in three domains, i.e., the spatial domain, frequency domain and compressed domain.

This paper illustrates various data hiding techniques to enable the safe transfer of critical data over the unsecure network. Vector quantization (VQ) has widely been used for signal processing.This is due to its excellent compression performance. Data hiding techniques in the VQ-compressed domain can relish advantages of both data hiding and compression for a multimedia distribution achieving a secure channel and bandwidth/space saving for data transmission/storage.

In general, reversible data hiding schemes and irreversible data hiding schemes are the two classifications of data hiding techniques. For irreversible data hiding schemes, only secret data can be extracted and cover images cannot be restored . Conversely, reversible data hiding schemes can extract the secret data and recover the original cover images simultaneously. An information hiding system is characterized using four different aspects: capacity-which is the amount of information that can be hidden in the cover medium, security-which refers to the inability of the hacker to extract hidden information from the cover image ,then perceptibility and robustness.

Stegnography is sometimes confused with cryptography, but there are some distinctive differences between the two. In some cases steganography is often refered as cryptography because in cryptography the cipher text is a scrambled output of the plaintext and the attacker can guess that encryption has been performed and hence can employ decryption techniques to acquire the hidden data. Also, cryptography techniques often require high computing power to perform encryption which may pose a serious hindrance for small devices that lack enough computing resources to implement encryption.

On the contrary, steganography is the process of hidding the sensitive information in any cover media like still images, audio, video over the internet. This way the attacker does not realize that the data is being transmitted since it is hidden to the naked eye and impossible to distinguish from the original media .In this paper we present a survey on various data hiding techniques along with their comparative analysis.

II. LITERATURE SURVEY

In this section we will be presenting the survey on various data hiding techniques to facilitate secure data transmission over communication network.

A. Reversible Data Hiding by Histogram Shifting

The histogram shifting technique utilizes zero or minimum point of histogram to hide the secret data. If the peak value is lower than the zero or minimum point in the histogram, then add pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding data, the complete image is searched. When we encounter a peak-pixel value , if the bit to be embedded is '1' the pixel is added by 1, else it is kept unchanged. Alternatively, if the peak is higher than the least point in the histogram, this method decreases pixel values by one from

lower than the peak to higher than the least point in the histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1. Similar to encoding, decoding process is also easy .Opposite of encoding process gives the decoding process.

The advantages of this method is that it includes higher simplicity, it always provide a constant PSNR 48.0dB. This technique offers a very low distortion and the embedding capacity is very high.

The disadvantages of this histogram shifting technique is the low capacity that is, the capacity is limited by the frequency of peak-pixel value in the histogram, and it searches the image several times, thus it consumes a lot of time.

B. Data Embedding Using Difference Expansion

This approach make use of a high quality reversible watermarking method with high capacity based on difference expansion. Here data embedding is done using pixel differences; this is because of the possibility of high redundancies among the neighbouring pixel values in natural images.

During embedding process , differences of neighbouring pixel values are calculated. In that differences the changeable bits are determined and some differences are selected to be expandable by 1-bit, thus the changeable bits increases. Then concatenated bit-stream of compressed original changeable bits. The location of increased difference numbers and the hash of original image is embedded into the changeable bits of difference numbers in a random order. The watermarked pixels are achieved by using inverse transform to from resultant differences.

During watermark extraction, differences of neighbouring pixel values are measured. Then we determine changeable bits in that calculated differences. Extract the changeable bit-stream ordered by the same pseudo random order as embedding, separate the compressed original changeable bit-stream, the compressed stream of bits of locations of expanded difference numbers , and the hash of original image from extracted bit-stream, decompress the compressed separated bit-streams and reconstruct the original image replacing the changeable bits calculate the hash of reconstructed image and compare with extracted hash.

The technique contains the following advantages .There is no loss of data due to compression decompression, this is also applicable to audio and video data. The encryption of compressed location map and changeable bit-stream of different numbers increases the security.

The disadvantages included in difference expansion are there may be some round off errors. The method largely sensitive to the smoothness of the image. So this method cannot be applied to textured images, whose capacity will be very low or even zero. There is significant degradation of visual quality due to replacements of bits of gray scale pixels.

C. Data Hiding By Simple LSB Substitution

This techniques is based on evaluating the least significant bit. This approach manipulate the least-signifcant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods achieves high embedding capacity. Optimal pixel adjustment processcan be applied to the stego-image which is obtained by the simple LSB substitution method, the quality of the image can be improved greatly. This can be achieved with low extra computational complexity.

LSB substituted data hiding in images is based on random substitution of bits which not only improves the robustness and security of the watermarking scheme but also significantly improves the stego image quality which is similar to that of the original cover image.

LSB substituted image is most affected by Gaussian noise .But this approach has good sustainability against salt & pepper noise. The main disadvantages of LSB substitution is the low embedding capacity of secret data into the cover image.

D. Data hiding Based On Search Order Coding for VQ Compressed Images

Vector Quantization is a popular and commonly used digital image compression technique. Since VQ significantly reduces the size of an image to a great extend, the technique can save the costs of storage space as well as image delivery. This method uses Search-Order Coding (SOC) to manipulate the randomly distributed histogram of a VQ-compressed image into locations close to zero. Then uses the encoding strategies to perform encoding and data hiding simultaneously. During encoding process, indicator is not required for indices to identify index types, which in turn helps improve compression performance.This technique can completely restore the VQ-compressed image after secret data extraction.

A novel reversible SOC-based data-hiding scheme is used to increase embedding capacity. The embedding capacity of image is increased and achieve lossless reconstruction of the cover image by using the help of SOC and hiding strategies. This technique applies SOC to a VQ-compressed image in order to achieve SOC compressed image, which can support higher capacity to embed data. During encoding process, SOC indices are modified to hide secret information and no indicator is required, and thus a low bit rate and a high embedding capacity can be obtained. In extraction process, the algorithm extracts the secret data as well as the cover image with good quality.But this technique is time consuming due to the complexity of the algorithm.

E. Information Hiding Based on Block Match Coding for VQ-Compressed Images

This method is an effective data hiding technique in which secret data is embedded into compressed image. These compressed images can be recovered without any loss after the secret data is extracted at the decoder. Vector Quantization (VQ) technique is used for compressing the image. Vector quantization involves index modification and side match vector quantization techniques to hide data. SMVQ technique can provide high embedding capacity and low bit rate but it is more complex and time consuming. In addition, data hiding done by index modifying technique provides only low embedding capacity and high bit rate .But this is more simple and less time consuming. So in this approach , the advantages of the two techniques are merged while removing the limitations. Thus scheme has the following characteristics: Complete recovery of the original cover image after the extraction of secret data, very high embedding capacity, high embedding rate, and limited time consuming. With the help of prediction index codebook is generated efficiently.Thus the encoding/hiding process can be easily accomplished using the codebook with simple calculation rather than a table lookup. The execution time of colour image (size 256 X 256) is 1.09 ms and (size 512 X 512) is 0.89 ms. The execution time of grayscale image (size 256 X 256) is 0.89 ms and (size 512 X 512) is 0.85 ms. The PSNR obtained is above 30dB. The size of the original image and output embedded image is same i.e size ratio of original image and output embedded image is nil.

III. COMPARISON

TABLE I
PERFORMANCE COMPARISONS

Parameters	Data Hiding Techniques				
	Simple LSB Substitution	Difference Expansion	Histogram Shifting	Search Order Coding for VQ	Block Match Coding for VQ
EC	Low	Low	Moderate	Moderate	High
BR	High	Moderate	Moderate	Low	Low
ER	Low	Moderate	Moderate	Moderate	Moderate
PSNR Value	≈ 32	≈ 36	≈ 42	≈ 45	≈ 46
Time Consuming	Less	Less	Less	More	More
Complexity	Low	Low	Moderate	High	High

IV. CONCLUSION

Data hiding techniques is getting popular due of the importance in securing secret data from unauthorised users or attackers. In this paper five different types of data hiding techniques for digital images: Simple LSB substitution technique, Difference expansion technique, Histogram modification technique ,Search order coding technique and Block match coding technique are studied, analyzed and compared. Parameters like embedding capacity, bit rate, embedding rate etc are used to compare the performance of different techniques. Most of the techniques discussed are reversible. Reversible data hiding techniques achieves real reversibility that is the cover image can be extracted completely at the decoder.The survey results show each technique has its own advantage and disadvantages.

REFERENCES

[1] Yaw-Hwang Chiou, Jiann-Der Lee, "Reversible Data Hiding Based on Search-order Coding for VQ-compressed" Journal of Convergence Information Technology(JCIT)Volume6, December 2011.
[2] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding" , IEEE transactions on circuit and systems for video technology, VOL. 16, NO. 3, March 2006
[3] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution" , City University of Hong Kong accepted 11 August 2003.
[4] Jiann-Der Lee, *Senior Member, IEEE*, Yaw-Hwang Chiou, and Jing-Ming Guo, "Information Hiding Based on Block Match Coding Vector Quantization-Compressed Images", IEEE systems journal, VOL. 8, NO. 3, September 2014
[5] Chin-Chen Chang, *Fellow, IEEE*, Yi-Pei Hsieh, and Chih-Yang Lin, "Lossless Data Embedding With High Embedding Capacity Based on Declustering for VQ-Compressed Codes", IEEE transactions on information forencics and security, VOL. 2, NO. 3, September 2007.
[6] Nilam R. Bagul, "Secure Information Hiding Using Block Match Coding For VQ - Compress Images", International Journal of Research and Engineering Vol.01.
[7] Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE transactions on circuits and systems for video technology, VOL. 13, NO. 8, August 2003.
[8] Chin-Chen Chang , Guei-Mei Chen, Min-Hui Lin, " Information hiding based on search-order coding for VQ indices", 18 May 2004 .
[9] G. Boopathy S. Arockiasamy " Implementation of Vector Quantization for Image Compression", GJCST Computing Classification.,22Vol.10,Issue3,April2010.
[10] Thai-Son Nguyen , Chin-Chen Chang, and Meng-Chieh Lin , " Hiding Scheme for SMVQ-Compressed Images using SOC Coding", Smart Computing Review, vol. 4, no. 3, June 2014.