Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Image Compression and Steganography Techniques

Chetan[1], Deepak Sharma[2]

[1]M.Tech Department of Information Technology

[2]Asst. Professor Department of Computer Science and Engineering

[1, 2] Adesh Institute of Engineering and Technology, Faridkot, Punjab, India

Abstract: Image compression is a technique to minimize the size in bytes of a graphics file without degrading the quality of image to an unacceptable level. On the other hand, steganography deals with embedding secret data in redundancies of image in invisibility manner. The goal of this study is to improve image compression through steaganography. Image compression addresses the problem of reducing the amount of data required to represent a digital image. It is a process intended to yield a compact representation of an image, thereby reducing the image storage/transmission requirements. The main use of our paper is to increase the image compression rate using steganography and the most effective compression algorithms.

Keywords: image compression, Steganography

I. INTRODUCTION

Compression is a process by which the description of computerized information is modified so that the capacity required to store or the bit-rate required to transmit it is reduced. Compression is carried out for the following reasons as to reduce, the storage requirement, processing time and transmission duration. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of image. Many applications need large number of images for solving problems. Digital images can be stored on disk, and storing space of image is important. Because less memory space means less time required for processing of image. Image Compression means reducing the amount of data required to represent a digital image.

Image Compression is achieved by removing the redundancy in the image. Redundancies in the image can be classified into three categories; inter-pixel or spatial redundancy, psycho-visual redundancy and coding redundancy.

Inter-pixel Redundancy: Natural images have high degree of correlation among its pixels. This correlation is referred as inter-pixel redundancy or spatial redundancy and is removed by either predictive coding or transform coding.

Psycho-visual redundancy: Images are normally meant for consumption of human eyes, which does not respond with equal sensitivity to all visual information. The relative relevancy of various image information components can be exploited to eliminate or reduce any amount of data that is psycho-visually redundant. The process, which removes or reduces Psycho-visual redundancy, is referred as quantization. .

Coding redundancy: variable-length codes matching to the statistical model of the image or its processed version exploits the coding redundancy in the image.

II. STEGANOGRAPHY

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means “cover writing”. Generally steganography is known as “invisible” communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today’s steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information.

Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

- **Steganography in Digital Mediums**

  Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

  i. Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

ii. Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields .

iii. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.,* 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

iv. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or *etc* for steganography.

v. Text Steganography: General technique in text steganography, such as number of
Tabs, white spaces, capital letters, just like Morse code and *etc* is used to achieve information hiding.

- **Image Steganographic Techniques**

Image steganography techniques can be divided into following domains.

i. Spatial Domain Methods: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

General advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

ii. Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

iii. Distortion Techniques: Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [18].Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit [19].The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a “1.” otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

iv. Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:

1. Techniques can be applied only to gray scale images and restricted to 24 bits.

III. LITERATURE REVIEW

- In [1] authors proposed an introduction of image processing, types of images, image processing operations, image segmentation.
- In [2] authors purposed an idea of image compression and its algorithms.
- In [3] authors Bernd Meyer and Piter Tischer proposed an idea of lossless grayscale image compression, TMW, that is based on the use of linear predictors and implicit segmentation to achieve compression.
- in [4] LOHIT M.KADLASKAR author purposed an idea of compression and decompression of raw image based on Huffman coding and reduce the memory space as compared to original image.
- In [5] authors purposed an idea of compress and decompress the image using steganography by using DCT JPEG and DWT JPEG. In this firstly author compressed and decompressed the image using DCT by dividing eight into eight block size then done embedding and vice versa then compression and decompression is done with the help of DWT.
- In [6] author purposed an idea of analysis of tampered image and image steganlysis and analysis different characteristics of DWT coefficients ,frequency histogram under single and double compression of post compression rate distortion optimization algorithms.
- [7] Pallavi M.sune author purposed an idea of conversion of an image into array using Delphi image control tool. They can be used to display a graphical image icon, Bitmap, GIF, JPEG etc then algorithm is created in Delphi to implement Huffman coding.
- In [8] authors purposed an idea of Fractal image compression can be obtained by dividing the original grey level image into unoverlapped blocks depending on a threshold value and the well known techniques of Quad tree decomposition. By using threshold value of 0.2 and Huffman coding for encoding and decoding of the image.
- In [9] authors purposed an idea of wavelet transform domain divided into different multi resolution and multi level sub bands, so quantization coding strategy singular value truncating were introduced. It mainly performs rearrangement on low frequency sub bands coefficient of wavelet image.
- In [10] authors purposed an idea of Image compression is a technique to minimize the size in bytes of a graphics file without degrading the quality of image to an unacceptable level. On the other hand, steganography deals with embedding secret data in redundancies of image in invisibility manner. The goal of this study is to improve image compression through steaganography using DCT & DWT.
- In [11] authors proposed an idea of combination of steganography and encryption algorithms, which provides a strong backbone for its security. The proposed system not only hides large volume of data within an image, but also limits the perceivable distortion that might occur in an image while processing it. This software has an advantage over other information security software because the hidden text is in the form of images, which are not obvious text information carriers.

IV. CONCLUSION AND FUTURE WORK

This paper gave an overview of image compression and different steganographic techniques its types and literature review based on image compression and steganography which have been proposed in the literature during last few years. We have analyzed different proposed techniques which show the visual quality of image.

REFERENCES

[1] Amandeep Kour, “a review on image processing (2013)”, international journal of electronics communications and computer engineering, vol 4

[2] Sachin Dhawan, “A review of image compression and comparison of its algorithms (2011)” , vol 2 issue1, international journal of electronics& communications technology.

[3] Bernd Meyer, Peter Tischer, “TMW – a new method for lossless image compression (2009).

[4] LOHIT M.KADLASKAR, “A new lossless method of image compression and decompression using Huffman coding techniques”. Journal of theoretical and applied information technology.

[5] REZA Jafari, Ziou, Mohammad mehdi rashidi, “increasing image compression rate using steganography (2013)”ELSEVIER.

[6] WANG WEI, WANG Rang –ding, “the analysis and detection of double jpeg2000 compression based on statistical characteristics of DWT (2012)” ELSEVIER.

[7] Pallvi M.sune, “image compression techniques based on wavelet and Huffman coding (2013)”, international journal of advanced research in computer science and software engineering.

[8] Veenadevi.S.V. And A.G.Ananth, "FRACTAL IMAGE COMPRESSION USING QUADTREE DECOMPOSITION AND HUFFMAN CODING (2012)" Signal & Image Processing: An International Journal (SIPIJ) Vol.3.

[10] Archna parkhe, "enhancing the image compression rate using steganography (2014)", The International Journal of Engineering and Science (IJES).

[11] Meenu Kumari, "JPEG compression steganography & cryptography using Image Adaption Technique (2010)", Journal of Advance in Information Technology.

[12] Rafael C. Gonzalez, Richard e woods "digital image processing", second Edition PAGE 410.

[13] Jain, fundamentals of digital image processing, prentice-hall Inc, 1982.

[14] Springer, digital image processing, bred jahne, 5th edition.