Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-02-31

Review of FPGA Based Data Hiding Data in Digital Images

Dr. Harsh Vikram Singh[1*], Ms. Suman Yadav[2] and Prof. Anand Mohan[3]
[1] Assistant Professor, [2] Research Assistant,
Department of Electronics, Kamla Nehru Institute of Technology, Sultanpur, India
[3] Director, National Institute of Technology, Kurukchetra, India

Abstract.

In recent years, the applications about multimedia have been developed rapidly. Digital media brings about conveniences to the people, because it is easy to be processed. At the same time, it enables the illegal attackers to attack the works. For the protection of data, there has been growing interest in developing effective techniques to discourage the unauthorized duplication of digital data. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The ultimate objective of the research presented in this paper was to develop low-power, high- performance, real-time, reliable and secure watermarking systems, which can be achieved through hardware implementations. In this paper, we present a review of FPGA based implementation of watermarking encoder and decoder.

Key Word: Field Programmable Gate Array (FPGA); Watermarking; Invisible algorithm; multimedia.

1 Introduction

The rapid expansion of the Internet and the overall development of digital technologies in the past years have sharply increased the availability of digital images. It is, therefore, very important to have the capabilities to detect copyright violations, and to control access to digital media when transmitting sensitive data over an insecure channel. Fueled by these concerns, data hiding has evolved as an emerging technology that enables the insertion of secret information invisibly throughout the image without degrading its visual quality. The potential applications of data hiding in digital images are steganography, watermarking, tamper detection, tamper proofing and fingerprinting.

Steganography is the art and science of hiding messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. In this project, we have implemented the concept of steganography with a FPGA IP core where digital images were selected as the cover media. After embedding the secret messages the images are called stego-images. The image-quality in data hiding is simply refers to the quality of these stego-images.

It is a well-known fact that unprotected digital content can be used to made unlimited number of duplicates of the original content. This issue motivated the digital media users and owners to secure the copyrights in a digital form. Data hiding showed them a good way of achieving that goal. In addition to that the digitized multimedia formats introduced a new problem. Normally, the form of the data

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-02-31

does not have significant impact on multimedia contents such as video or audio. The visible or audible information can be converted into other formats. They can even pass through analog connections without significant distortion to the contents. This issue also requested suitable method to be used in digital data manipulating systems to secure the content. Steganography is one such method used in digital information handling.

In order to have good stego-image, it should satisfy few general requirements. First, the embedded data should be directly encoded into the media, rather than into a header or wrapper. Also, the embedded data should not be visible in the image under typical viewing (Human Visual Systems). This is also referred to as imperceptibility. Also, it must be capable of allowing large amounts of data being embedded in an image. Furthermore it should conceder about the efficiency of the transmission of the covering media. There are lots of techniques proposed to balance the tradeoff between them. One such technique is the LSB substitution method together with Optimal Pixel Adjustment Process.

Data Hiding Properties:

Digital data hiding is characterized with the following properties:-

1. Unobstrusive : The watermark should be perceptually invisible to the viewer nor should the watermark degrade the quality of the content.

2. Robustness: The watermark must be difficult to remove. In particular, the watermark should be robust to the attacks.

3. Universality: The same digital watermark algorithm should apply to all three media types viz. audio, video and image.

4. Tamper-resistance: The watermarking techniques should be robust to legitimate signal distortions as well as intentional attacks to remove or tamper with the digital watermark.

5. Common Signal Processing: The watermark should still be retrievable even if common signal processing operations are applied to the data.

6. Common Geometric Distortions: Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping, and scaling.

7. Subterfuge Attacks, Collusion and Forgery: the watermark should be robust to combining copies of the same data set to destroy the watermarks.

Characteristics of Watermarks

Images are the best steganography due to their high embedding capacity eg. An image consisting 1024 x 1024 pixels has about 1 Mpixel; each can represent 256 colours using 8-bits. If, however, the colour pixels are represented by 24-bits ,this can provide more space for hiding information. Further, still images being non-causal offer additional benefit when used as cover.

Although embedding messages into an image is an attractive technique for data hiding, it has a major limitation due to large data overhead, which necessitates use of compression techniques for storage and transmission of stego images. [5]

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-02-31

The commonly used carriers are : network protocols (TCP,IP and UDP), digital audio(MPI,MPEG,MIDI,WAV,AVI and VOC),text files (JAVA,HTML) and color / grey-scale image files(JPEG,TIFF,GIF and BMP). [6]

JPEG: The term "JPEG" is an acronym for the Joint Photographic Experts Group. In computing, JPEG is a commonly used method of lossy compression for digital photography . The degree of compression can be adjusted, allowing a selectable trade-off between storage size and image quality. JPEG typically achieves 10:1 compression with little perceptible loss in image quality. It supports a maximum image size of 65535×65535. [7]

Watermarking Techniques:

In recent years, the advancement in the field of steganography has led to the following steganographic techniques:

1. SPATIAL DOMAIN ALGORITHMS: Spatial domain digital watermarking algorithms directly load the raw data into the original image.It is of following types:-

(a) Least Significant Bits Insertion-

This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in a JPEG image for example, the following steps would need to be taken :

- First load up both the host image and the image you need to hide.
- Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.
- Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001

Secret Pixel: 00111111

New Image Pixel: 10110011

- To get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

Host Pixel: 10110011

Bits used: 4

New Image: 00110000

The major limitation of this technique is its sensitivity to filtering or manipulations (on stego -object) and weak resistance to tampering i.e. an attacker can easily destruct secret message simply by removing or zeroing the entire LSB plane without any noticeable change in the perceptual quality of the modified stego-object. [11]

(b) Patchwork algorithm

Based on the statistics, the algorithm uses the statistical characteristics of pixels to

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-02-31

embed the information into the brightness values of pixel. It can resist lossy compression coding and malicious attacks. However, the amount of embedded information is limited, in order to embed more watermark information; we can segment the image, and then implement the embedding operation each image block. [9]

(c) Texture mapping coding method

It hides the watermark in the texture part of the original image. The algorithm has strong resistance ability to attacks for a variety of deformation, but only suitable for areas with a large number of arbitrary texture images, and cannot be done automatically. [9]

2. TRANSFORM DOMAIN EMBEDDING

Transform domain embedding is achieved using DCT or Wavelet Transform in majority situations; however, in some cases FFT may also be used [10]. In this case data are mainly, Embedded into high frequency components of the image to have lesser effect on the image quality. The amount of embedded data is adaptively varied according to the local characteristics of the original image. If the data is embedded uniformly into all pixels or all DCT coefficients are computed from pixels without accounting for the local characteristics of the image or into low frequency components of image, this tends to introduce outstanding distortion in the stego –image such as rough patterns, blurred edges and degradation of colours.

$$F(u)=C(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

$$where\ u=0,1,\ldots N-1$$

$$C(u)=\sqrt{\frac{1}{N}}\ when\ u=0 \quad C(u)=\sqrt{\frac{2}{N}}\ when\ u\neq 0$$

3. SPREAD SPECTRUM

Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium. The message is spread over wide bandwidth that has poor SNR in every band making it difficult to detect. Further, even if parts of the message are tampered or removed from several bands, still information present in the other bands can be utilized to recover the original message. Therefore, it is difficult to remove the message completely without destroying the cover and thus it is a robust technique.

Conclusion:

The proliferation of network multimedia systems dictates the need for copyright protection of digital property. Future work will concentrate on producing watermarks that are robust to filtering, lossy image compression, noise corruption and changes in contrast. This paper serves as a brief summary on several more recent and popular digital watermarking techniques for multimedia information systems.

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-02-31

Acknowledgements

The authors gratefully acknowledge financial support from the Council of Science & Technology, Government of Uttar Pradesh (INDIA) under young scientist scheme.

References

[1] Johnson N.F and Jajodia S.: 'Exploring Steganography: Seeing the unseen,' *IEEE Computer*, 1998, vol.31, no.2 pp.26–34.

[2] Fridrich J.: 'Steganography in Digital Media Principles, Algorithms and Application', Cambridge University Press, 2010, New York.

[3] Cheddad A., Condell J., Curran K. and M Kevitt P.: 'Digital image Steganography: Survey and analysis of current methods', Review Article, *Signal Process.*, 2010, vol. 90, pp.727-752.

[4] Chang C.C., Chung J.C.: 'An image intellectual property protection scheme for gray-level images using visual secret sharing strategy', *Pattern Recognit. Letters*, 2002, vol.23, pp.931–941.

[5] Hsieh S.L., Huang B.Y.: 'A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation'. Proc. Int. Computer Symposium, 2004, pp. 661–666.

[6] Hsu C.S., Hou Y.C.: 'Copyright protection scheme for digital images using visual cryptography and sampling methods', *Optical Engg.*, 2005, vol. 44, pp.077003.

[7] Wang S.H., Lin Y.P.: 'Wavelet tree quantization for copyright protection watermarking', *IEEE Trans. Image Processing*, 2004,vol. 13, no.2, pp.154–165.

[8] Liu R, Tan T.: 'An SVD-based watermarking scheme for protecting rightful ownership', *IEEE Trans. Multimedia*, 2002, vol.4, no.1, pp.121–128.

[9] Bhatnagar G., Raman B.: 'A new robust reference watermarking scheme based on DWT-SVD', *Comput. Stand. Interfaces*, 2009, vol.31, pp.1002-1013.

[10] Wang M.S., Chen W.C.: 'A hybrid DWT-SVD copyright scheme based on K-mean clustering and visual cryptography',*Comput. Stand. Interfaces*, 2009, vol.31, pp.750-762.