ISSN (ONLINE):2045-8711
ISSN(PRINT): 2045-869x

International Journal of Innovative Technology & Creative Engineering

July - 2014
Vol.4 No.7

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering 1a park lane,
Cranford
London
TW59WA
UK
E-Mail: editor@ijitce.co.uk
Phone: +44-773-043-0249

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.
Phone: 001-706-206-0812
Fax:001-706-542-2626

India: Editor
International Journal of Innovative Technology & Creative Engineering
Dr. Arthanariee. A. M
Finance Tracking Center India
17/14 Ganapathy Nagar
2nd Street
Ekkattuthangal
Chennai 600032
Mobile: 91-7598208700

www.ijitce.co.uk

IJITCE PUBLICATION

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING

VOL.4 NO.7

July 2014

www.ijitce.co.uk

EDITORIAL MEMBERS

CONTENTS

Safe communication using Data-hiding method based on Image Steganography and Cryptography

#1 Mrs.B.Sindhupiriyaa, #2 Mrs.R.Sasiregha
#1 Department Of Computer Science, SSM College of Arts & Science,
#2 Assistant Professor, Department Of Computer Science,
SSM College of Arts & Science, Komarapalayam – 638 183, India.
#1 sindhutbharathi@gmail.com

Abstract- This paper describes adaptive mechanisms for high-volume transform-domain data hiding in MPEG-2 Image which can be tuned to sustain varying levels of compression attacks. The data is hidden in the uncompressed domain by scalar quantization index modulation (QIM) on a selected set of low-frequency discrete cosine transform (DCT) coefficients. Information-theoretic analyses for data hiding prescribe embedding the hidden data in the choice of quantize for the host data. In this paper, we propose practical realizations of this prescription for data hiding in images, with a view to hiding large volumes of data with low perceptual degradation. Our embedding scheme incurs insertions and deletions at the decoder which may cause de-synchronization and decoding failure. This problem is solved by the use of powerful turbo-like codes and erasures at the encoder. The channel capacity estimate gives an idea of the minimum code redundancy factor required for reliable decoding of hidden data transmitted through the channel. We apply multilevel embedding to allow the amount of embedded information that can be reliably extracted to be adaptive with respect to the actual noise conditions. When extending the multilevel embedding to Image, we propose strategies for handling uneven embedding capacity from region to region within a frame as well as from frame to frame.

Keywords: *Image Data Hiding, Multilevel Embedding, Digital Watermarking, Embedding Capacity.*

I. Introduction

This paper describes a few fundamental issues of data hiding in image. This paper proposed general solutions, including how to embed multiple bits, how to handle uneven embedding capacity, and how to allow the number of reliably extractable bits to be adaptable to the actual noise condition. Here in Part-II, we apply the solutions to specific design problems and present details of embedding data in image and image. In Section II, we embed data in images at two levels, each of which is designed for different robustness. This approach allows for graceful decaying of extractable information as noise gets stronger. In Section III, we extend the multilevel embedding to image, for which difficulty arises because the embedding capacity varies from region to region within a frame as well as from frame to frame. We embed control information to facilitate the extraction of the user data payload and to combat such distortions as frame jitter. The designs presented in this paper can be used as building blocks for such applications as copy control, access control, robust annotation, and content-based authentication.

Comprehensive protection from malicious attacks that make watermarks undetectable would require both technical and business approaches, such as a well-determined business and pricing model. Our design objective here focuses on surviving common processing in transcoding and scalable/progressive transmission, such as compression with different ratio and frame rate conversion for image.

However, most of the image data hiding methods utilize uncompressed image data. Sarkar *et al.* [2] proposed a high volume transform domain data hiding in MPEG-2 images. They applied quantization index modulation (QIM) to low frequency DCT coefficients and adapted the quantization parameter based on MPEG-2 parameters. Furthermore, they varied the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes de-synchronization. They utilized repeat accumulate (RA) codes in order to withstand erasures. Since they adapted the parameters according to type of frame, each frame is processed separately. RA codes are already applied in image data hiding. In [3], adaptive block selection results in de-synchronization and they utilized RA codes to handle erasures. Insertions and erasures can be also handled by convolutional codes as in [4]. The authors used convolutional codes at embedded. However, the burden is placed on the decoder. Multiple parallel Viterbi decoders are used to correct de-synchronization errors. However, it is observed [4] that such a scheme is successful when the number of selected host signal samples is much less than the total number of host signals samples.

II. Background Work

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered. *Vot 71847 Information Hiding using Steganography Approach* The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, image, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly.

Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Some of the techniques used in steganography are domain tools or simple system such as least significant bit (LSB) insertion and noise manipulation, and transform domain that involve manipulation algorithms and image transformation such as discrete cosine transformation and wavelet transformation. However there are technique that share the characteristic of both of the image and domain tools such as patchwork, pattern block encoding, spread spectrum methods and masking.

Based on the embedding domain, the existing image steganography methods can be classified into spatial domain and transform domain methods. Spatial domain methods embed the secret data directly embedded into pixels of the cover image. The two most widely used spatial domain steganography techniques are the Least Significant Bit (LSB) and Bit Plane Complexity Steganography (BPCS) technique [4-7]. In LSB technique, the LSB of cover image are replaced by embedded bits. In BPCS the cover image is divided into blocks and classified into information and noisy blocks, the secret data is hidden into noisy blocks. These techniques are computationally simple and straightforward but are more fragile to external attacks and, therefore, less robust. Transform domain methods, also known as frequency domain, first transform the cover image into a set of frequency domain coefficients using Fourier transform, Discrete Cosine Transform (DCT) or wavelet transform. The secret data is then embedded in transformed coefficients. Transform domain methods require more computations but are robust against common image processing operations such as existing image compression standards (JPEG, MPEG, JPEG2000, etc.), low-pass filtering, cropping, and addition of noise [9]. Steganography using DFT requires encoding of both magnitude and phase information of image and is not compatible with the international data compression standards such as JPEG and MPEG whereas DWT is not popular for JPEG and MPEG compression of image/image files. Due to relatively low computational complexity and compatibility with the international data compression standards like JPEG and MPEG, DCT domain steganography technique is widely used. There a number of publicly available steganography tools that embed data by modifying DCT coefficients including Jsteg [10], Outguess [11] and F5 [12]. Both Jsteg and F5 embed the data into the quantized DCT (Discrete Cosine Transform) coefficients of JPEG image. F5 permutes the DCT coefficients before embedding and employs matrix embedding. An improvement of coding method used in F5 is proposed by Fan et al. [13]. Outguess also embeds data by flipping LSBs of DCT coefficient, but it spreads out changes by selecting coefficients with the user-selected password [14]. An extensive survey of digital image steganography can be found in [15].

III. Methods - Genetic Algorithm

Genetic Algorithm is a technique which mimics the genetic evolution as its model to solve problems. The given problem is considered as input and the solutions are coded according to a pattern. The *fitness* function evaluates every candidate solution most of which are chosen randomly. Evolution begins from a completely random set of entities and is repeated in subsequent generations. The most suitable, and not the bests, are picked out in every generation. Our GA aims to improve the image quality. Pick Signal to Noise Ratio (PSNR) can be an appropriate evaluation test.

IV. Result Analysis - Conclusion

A novel approach of hiding image in selected image sequence based on their mean square error rate has been proposed in this paper, which works through the technique of hybrid image-hiding scheme based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). A number of fundamental problems of data hiding have been investigated and solutions proposed. The analysis of the tradeoff of embedding capacity versus robustness for two major types of embedding mechanisms leads to a new, multilevel data embedding framework, which allows the amount of extractable data being adaptive to the actual noise condition. We have also studied the suitable conditions of using various modulation/multiplexing techniques for hiding multiple bits. Finally, we proposed solutions to the problem of unevenly distributed embedding capacity.

References

[1] M.Wu, H.Yu, and B. Liu, "Data hiding in image and image: Part II—Designs and applications," *IEEE Trans. Image Processing*, this issue.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Mateo, CA: Morgan Kaufmann, 2001.

[3] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking," *EURASIP J. Appl. Signal Process.*, vol. 2002, no. 2, pp. 126–132, Feb. 2002.

[4] F. Mintzer, G.W. Braudaway, and M. M. Yeung, "Effective and ineffective digitalwatermarks," in *IEEE Int. Conf. Image Processing (ICIP'97)*, 1997.

[5] R. J. Anderson and F. A. P. Petitcolas. (1999) Information Hiding: An Annotated Bibliography. [Online]. Available: http://www.cl.cam.ac.uk/ ~fapp2/ steganography/ bibliography/

[6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," *Proc. IEEE*, pp. 1062–1078, July 1999.

[7] F. Hartung and M.Kutter, "Multimediawatermarking techniques," *Proc. IEEE*, pp. 1079–1107, July 1999.

[8] "Special issue on watermarking," *Signal Process.*, vol. 66, no. 3, May 1998.

[9] "Special issue on watermarking," *Commun. ACM*, vol. 41, no. 7, July 1998.

[10] "Copyright and privacy protection, special issue," *IEEE J. Select. Areas Commun.*, vol. 16, May 1998.

[11] "Special issue on identification and protection of multimedia information," *Proc. IEEE*, July 1999.

[12] W. Zeng, "Resilient Image Transmission and Multimedia Database Application," Ph.D. dissertation, Princeton Univ., Princeton, NJ, 1997.

[13] L. Qiao, "Multimedia security and copyright protection," Ph.D. dissertation, Univ. Illinois at Urbana-Champaign, 1998.

[14] M. Maes, T. Kalker, J. Haitsma, and G. Depovere, "Exploiting shift invariance to obtain a high payload in digital image watermarking," in *Proc. IEEE ICMCS*, vol. 1. Jul. 1999, pp. 7–12.

[15] T. Kalker, G. Depovere, J. Haitsma, and M. J. Maes, "Image watermarking system for broadcast monitoring," in *Proc. SPIE Security Watermarking Multimedia Contents Conf.*, vol. 3657. 1999, pp. 103–112.

[16] M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, F. G. Depovere, and J. Haitsma, "Digital watermarking for DVD image copy protection," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 47–57, Sep. 2000.

[17] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete image quality-preserving data hiding," *IEEE Trans. Circuits Syst. Image Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

[18] G. Tardos, "Optimal probabilistic fingerprint codes," in *Proc. 35th Annu. ACM STOC*, 2003, pp. 116–125.

[19] B. Skoric, T. U. Vladimirova, M. Celik, and J. C. Talstra, “Tardos fingerprinting is better than we thought,” *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3663–3676, Aug. 2008.