OFDM Based High Capacity Information Hiding in Grey Scale Image

Somnath Maiti, Abhik Roy, Tirtha Sankar Das, Subir Kumar Sarkar

Abstract— This paper proposes a robust information hiding method by utilizing the spectrum efficient OFDM technique applied on gray scale image onto another gray carrier image. For simplicity, the data mapping in complex domain we have used 4-QAM. A modified QIM technique for data embedding is used for improving robustness. But the robustness analysis is not a common practice for QIM based data hiding. The result shows a large amount of information hiding capability along with substantial improvement in robustness against intentional impairments. But the possibility of using OFDM technique in robust high capacity data hiding has drawn a very little attention to the researchers even today.

Index Terms— OFDM, QIM, QAM, Capacity, Robustness.

I. INTRODUCTION

The information concealment is basically used for copyright protection against infringement. Today's era is of broadband wireless communication meant for image and video transmission. So there is an increasing demand for high capacity robust information hiding technique as compared to the conventional low capacity robust method. We are proposing an approach to serve this purpose.

Generally, the data hiding techniques in transform domain can be divided into two broad categories .First one is Spread spectrum based , which offers best possible robustness against attack but it has very poor information hiding capacity, whereas the second method is based on QIM technique which shows higher information hiding capability but very poor in robustness. The robustness and data hiding capacity are two conflicting requirements. In this context, we addressed this issue in our proposed model as one of the best possible compromise between the two conflicting requirements.

Different techniques of Digital communication are being used by different researchers using model proposed by Cox. et al [1]. These models view the information hiding technique as basically a digital modulation and information retrieval as digital demodulation process. The only significant distinction is the carrier type i.e. a non-stationary system, which is an image called cover image for data hiding process whereas a pure sinusoid is used in digital CW modulation. The performance measure for data hiding techniques also plays important role to distinguish it from conventional digital modulation techniques.

Manuscript received December 09, 2011.

Somnath Maiti, ETCE Department, Jadavpur University, Kolkata 700032, sm_hit@rediffmail.com

Abhik Roy, ETCE Department, Jadavpur University, Kolkata 700032, abhikfiem@gmail.com

Tirtha Sankar Das, ETCE Department, RCC Institute of Information Technology, Kolkata 700015, tirthasankardas@yahoo.co.in

Subir Kumar Sarkar, ETCE Department, Jadavpur University, Kolkata 700032, su_sirsir@yahoo.co.in

An important criterion in this regard is the imperceptibility of the embedded image. This is also critically related to robustness of data hiding algorithm, the amount of information to be embedded and receiver operating characteristics (ROC).

OFDM is a popular broadband wireless technology. It is a multicarrier system uses discrete Fourier Transform/Fast Fourier Transform (DFT/FFT) spectra for subcarriers. Data is carried by varying the phase or amplitude of each subcarrier using either M-PSK or M-QAM .Parallel data streams mapped into complex numbers applied as the IFFT input, which results in modulation of the subcarriers. The output is the sum of many samples of many sinusoids and appears to be random. In effect, the modulation and multiplexing is performed in one step. Each subcarriers has a different frequency, chosen so that an integral number of cycles in a symbol period i.e. carriers are orthogonal. The key idea of utilizing OFDM in data embedding is its broad banding characteristics along with randomness of signal samples (coefficients).

B. Chen and G. W. Wornell [2], proposed quantization index modulation (QIM) and, through dither modulation (DM) and distortion compensation (DC) [3], improved their QIM watermarking. We tried to improve the basic scheme for QIM-based watermarking using OFDM.

Information hiding algorithms based on OFDM as proposed by Fan Tie-sheng et al. [7] have demonstrated the large capacity preposition information hiding onto a gray scale image Watermarking was proposed. The noticeable fact is that the robustness of data hiding is not justified through attack analysis. It was also claimed that the extraction method is blind though it directly requires the host image in terms of positional information of the relative luminance. Another similar work proposed by Mahalingam Ramkumar et al [13]. They have shown the BER performance against JPEG compression only. Jinhua Liu et al. [14] proposed watermarking algorithm based on Multiband Wavelet and Independent Component Analysis for Quantization Index Modulation. Experimental results showed the proposed algorithm has good robustness against JPEG compression, White Gaussian Noise only. A. Ouled Zaid et al [11] proposes integrated wavelet-based non-linear scaling QIM (NLS–QIM).Only the BER performance against Gaussian noise is analysed. Xianfeng Zhao et. al [15] proposed another scheme for improving robustness of QIM based watermarking by means of Non uniform Discrete Cosine Transform. They claimed to test their algorithm against JPEG, AWGN and various type of filtering but the result is not shown.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

We addressed all these issues with substantial improvement of robustness against intentional or unintentional impairments attack. This paper is organized in the following sections. The section-II explains the block diagram of embedding and extraction process. Section-III and section-IV details the functions of different sub units involved in the data concealment and detection procedure. Section-V discusses the computational complexity, and Section-VI discusses result of capacity, attack analysis and security measure. Finally, section VII concludes the paper.

II. EMBEDDING & DETECTION ARCHITECTURE

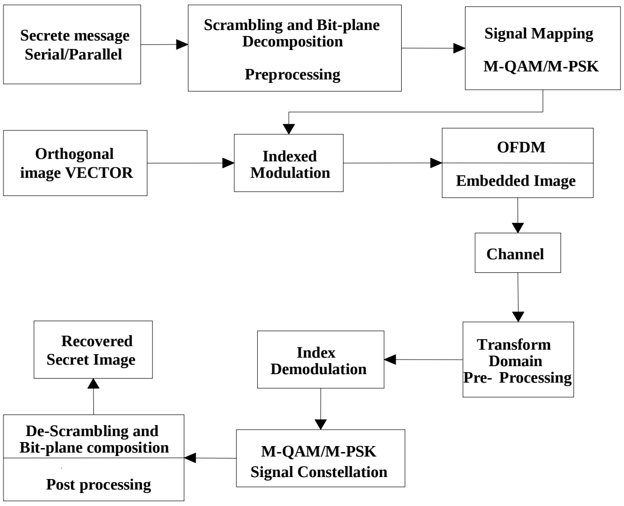

Fig.1 Detail block diagram of the proposed system.

The figure 1 shows the block diagram of the proposed system. The secret message is a gray scale image of size N x N is first scrambled to distribute energy evenly in space domain i.e. pixel location is changed. Next the Bit- plane decomposition is done for preparation to M-QAM/M-PSK mapping. After the mapping the data is mapped in complex domain. The data is now arranged in Conjugate symmetric pattern in order to retrieve data with real value. The cover image of size M x M is taken to transformed domain by applying FFT to form orthogonal image vectors. Suitable QIM technique [2, 3] is used for embedding Conjugate symmetric data into the transformed coefficients of cover image. The Indexed modulation scheme modifies Fourier coefficients of host coefficient index by the secret image coefficient indexes and then quantizing the host signal with associated quantizers. A quantizer maps a value to the nearest point belonging to a class of pre-defined discontinuous points. Here we change every transformed symbols of the host image block according to the secret information. The conventional OFDM is used by means of IFFT in order to reconstruct the embedded cover image.

III. EMBEDDING FUNCTIONAL SUBUNITS

The secret information we use is a binary image which acts as a secure signature. There is a growing demand of video watermarking in recent time, which demands high pay load capacity. As a part of our proposed approach of increasing pay load capacity, in the encoder we may scramble the secret message signal by applying Toral Automorphism. This is not to improve robustness but used as a soft key. Then QIM is applied as a visual data hiding algorithm to embed the secret message. Finally, we may follow the reverse procedure so that the hidden message can be recovered with subjective as well as objective perceptibility.

A. Scrambler: Toral Automorphism

A two dimensional "toral automorphism" can be consider as spatial transformation of planar regions [5]. It is depicted by the following equation (1):

$$A : U \to U = [0,1) \times [0,1) \in R^2 \qquad (1)$$

This method also has the ability to recover the original signal whenever reapplied on the scrambled image using a special type of private key. In the R dimensional space, the toral automorphism is given by the following formulae:

The special two dimensional case of toral automorphism is as follows:

$$C_n \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \qquad (2)$$

Where k [1, N] Z, (x, y) and x' are the pixel positions (of image) before and after the transform. If the chaotic mixing formula C_n has period P, (x, y) can return to the original position after P times of the C_n operation. Consequently, if the point (x, y) has been transformed T times using the C_n operation where T<P, it needs (P-T) transforms of the C_n operation to restore (x, y) back to the original position. From the point of view of encryption, using k and T as the encryption key, the related decryption key will be k and (P – T).

B. Bit plane Decomposition

There are various M-ary ASK & PSK schemes. As an example of M-QAM constellation, the 8-bit gray scale image is broken down into M planes, each containing symbols S (0, 1 2…M-1) by combining every log_2M bits of any pixel.

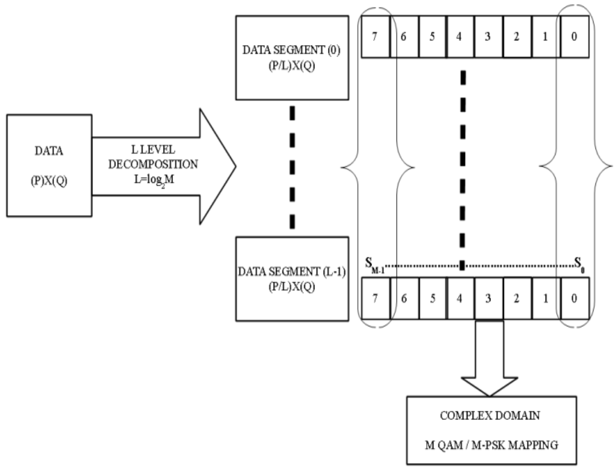

Fig.2 Schematic of Bit Plane Decomposition

C. Conjugate Symmetry

The gray scale image is represented by real integers. Therefore we need only the real values, and not the complex quantities. The problem is solved by augmenting the original sequence by appending its complex conjugate to it, as shown in Fig.2. The 2*N*-point IFFT of this augmented sequence is then a sequence of *2N* real numbers, which is equivalent in bandwidth to *N* complex numbers.

The augmented sequence is formed from the original sequence as

$$D_n^{'} = \begin{Bmatrix} D_n^{'} \\ D_{2N-n'}^{*} \end{Bmatrix} \begin{matrix} n = 1,\ldots N-1 \\ n = N+1,\ldots 2N-1 \end{matrix} \quad (3)$$

In order to maintain conjugate symmetry it is essential that D_0' and D_N' be real. If the original D_0 is zero then D_0' and D_N' are set to zero. Otherwise D_0' is replaced by **Re** (D_0) and D_N' to **Im** (D_0) [4].

D. Indexed Modulation

In our proposed scheme the original message signals are modulated by Δ/x factor, where Δ is step size and x is a positive integer which determines the robustness of our algorithm. Let 'w' is the Euclidian distance in the signal space. After it is modulated by Δ/x factor it becomes.

$$w^{'} = \frac{\Delta w}{x} \quad (4)$$

After QIM, let w' becomes w''.

$$w^{''} = \Delta round\left(\frac{c}{\Delta}\right) + w' \quad (5)$$

Where c is the FFT coefficient of carrier image. At the receiver end suppose we get the information bit as w'''.

IV. DETECTION FUNCTIONAL SUBUNITS

In the Decoding phase, a process akin to the reverse of QIM is performed on the stego image in order to estimate the subjectively recognizable visual information. The hidden symbols are detected by calculating the difference between the quantized and non-quantized stego signal coefficients. The symbols of MQAM/MPSK are estimated from these values and mapped correspondingly to their bit planes. An optimum quantization value is evaluated for a suitable subjective recognition. Since the decoder has no prior knowledge of the hidden information and the cover image, therefore the system has no reference. Following the reverse process of reassembling data in corresponding bit planes we get back the secret Information, which is a grey scale image. It does not resembling the original one because it is in the scrambled form. So we apply the toral automorphism once again over the same with the private key being used during encoding process and thus we are able to recover the secret Information. So using QIM demodulation we can write

$$w^{'''} = \Delta round\left(\frac{c}{\Delta}\right) + w^{'} - \Delta round\left(\frac{w''}{\Delta}\right) \quad (6)$$

Now to recover the information from w' which must be equal to w''. So we can write

$$\frac{\Delta w}{x} = \Delta round\left(\frac{c}{\Delta}\right) + w^{'} - \Delta round\left(\frac{w''}{\Delta}\right) \quad (7)$$

On simplifying the above equation we can write

$$round\left(round\left(\frac{c}{\Delta}\right) + \frac{w}{x}\right) = round\left(\frac{c}{\Delta}\right) \quad (8)$$

This will be satisfied if $w/x > 0.5$. For the above QIM method 'w' is equals to 1, therefore the robustness parameter is $x > 2$ in order to achieve the ROC criterion.

V. COMPUTATIONAL COMPLEXITY

We see that the total number of multiplication and addition can be expressed as, $42M^3 - 15M^2 + 9M^4 + M\left(24M^2 + 24M\right)$ where M is the size of the grey scale logo. Whereas, the computational complexity of the cover image due to one dimensional FFT operation is $O\left(N\log_2 N\right)$ where N is the size of the cover image. Therefore the overall computation complexity is $O\left(M^4\right) + O\left(N\log_2 N\right)$.

VI. RESULTS & DISCUSSION

A transformed domain high capacity data hiding algorithm is designed where the data is embedded in the quantized coefficients of grey scale host image. The imperceptible quality of the proposed algorithm has been estimated in terms of different objective quality matrices e.g. PSNR, UIQI, SSIM, AD, IF (Image fidelity), HS (Histogram Similarity) etc [6]. On the other hand the resiliency performance of the stego image is evaluated against various image distortions as well as noisy modulated signal similar to the concept of drift in oscillator carrier frequency in synchronous detection (in terms of e.g. NC (Normalized Cross-Correlation), CF (Correlation Factor), PCC (Pearson Correlation Coefficient), NHD (Normalized Hamming Distance), WDR (Watermark to Document Ratio) etc). It has been observed that the detected watermarks are quite subjectively recognizable even after a higher depth of degradations occurred in the embedded image. The experimental results of the imperceptibility, robustness and security performance are given in table 1, 2, 3 and 6. For security, lower the value better the data hiding capability. The results obtained from the proposed method are compared with some of the well established algorithms in terms of capacity, imperceptibility and robustness. Comparison results are presented in Table 4 & 5 respectively.

TABLE 1 ROBUSTNESS PERFORMANCE AGAINST AWGN NOISE.

Sl. No	Metric	Additive White Gaussian Noise (Mean = 1)Variance		
		5	*7.5*	*10*
1	NC	0.78163	0.66726	0.59361
2	CF	0.92637	0.86695	0.82046
3	PCC	0.54651	0.42352	0.32577
4	NHD	0.061523	0.1377	0.19287
5	WDR	-8.2781	-5.8662	-4.7334

TABLE 2 VISUAL QUALITY OF THE STEGO IMAGE SIGNAL (PART I).

Sl. No	Image	PSNR (dB)	UIQI	SSIM	AD	NAD
1	LENA	40.0344	0.9926	0.8870	2.9538	0.023904
2	FISHING BOAT	40.2651	0.9913	0.9067	3.2604	0.025137
3	U.S. AIR FORCE	39.4057	0.9935	0.8490	3.169	0.019319
4	HAT	40.3248	0.994	0.9187	3.1123	0.023776
5	CAMERAMAN	40.6790	0.996	0.8536	2.7915	0.023512

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

TABLE 3 VISUAL QUALITY OF THE STEGO IMAGE SIGNAL (PART II).

Sl. No	Image	MSE	NMSE	SNR(dB)	IF	HS
1	LENA	33.2042	0.0018902	27.2349	0.99811	6032
2	FISHING BOAT	37.4233	0.0019691	27.0574	0.99803	6470
3	U.S. AIR FORCE	34.9105	0.0011759	29.2961	0.99882	9326
4	HAT	36.4091	0.0018013	27.4441	0.9982	3088
5	CAMERAMAN	29.9692	0.0016666	27.7816	0.99833	9876

TABLE 4 THE PERFORMANCE RESULTS FOR IMPERCEPTIBILITY AND CAPACITY

Method	PSNR (dB)	Capacity (bits)
	Picture (Lena)	
Variable dimension Vector Quantization [2]	32.50	709 (64)
Vector Quantization [3]	32.62	4096 (512)
QIM-JPEG [4]	37.81	35304 (512)
Improved QIM-JPEG2000 [8]	34.90	4096 (512)
Vector Quantization [11]	32.25	-
Side-match Vector Quantization [11]	27.88	-
Paired Indexed Modulation [11]	29.54	16154 (512)
FSSM-QIM [11]	27.88	8065 (512)
Reversible QIM [11]	32.25	16256 (512)
Proposed OFDM-QIM	40.03	32768 (256)

TABLE 5 THE PERFORMANCE RESULTS FOR ROBUSTNESS (ON LENA)

Method	Low Pass	High Pass	AGNoise	JPEG	Crop
Vector Quantization [9]	0.99 (NC)	0.958 (NC)	-	0.876 (10%) (NC)	0.749 (NC)
Improved QIM-JPEG2000 [11]	-	-	0.1 (BER)	-	-
Proposed OFDM-QIM	0.68864 (CF)	0.6044 (CF)	0.9264 (CF)	0.951 (CF)	1 (CF)

TABLE 6 THE PERFORMANCE RESULTS FOR ROBUSTNESS (ON LENA)

Sl. No	Image	Security Value (Kullbeck-Leibler Distance)
1	LENA	0.0081
2	FISHING BOAT	0.0083
3	HAT	0.0023

VII. CONCLUSIONS

We have tested our proposed algorithm on the host image of size 256X256 and the grey scale information image of size 64X64. The proposed scheme achieves higher payload compared to the conventional methods as they basically embed binary bit streams. Moreover, this data hiding technique is able to retain a better degree of visual perception and also moderate robustness performances are achieved. The OFDM based QIM watermarking method finally improve its inherent deficiency against intentional and unintentional image impairments along with higher amount of embedding data.

Fig.3 Host Image

Fig.4 Watermark Image

REFERENCES

1. I.J. Cox, J. Kilian, F.T. Leighton et al, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, 1997 6 (12):167321687.
2. B.Chen and G.W.Ornell, "Quantization Index Modulation Methods for Digital Watermarking & Information Embedding of Multimedia", Journal of VLSI Signal Processing 27, 7-33, 2001.
3. B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", IEEE Trans. Inform. Theory.
4. Ahmed R.S. Bahai, Burton R. Saltzberg, Mustafa Ergan, "Multicarrier Digital Communications Theory and Applications of OFDM", Springer Science & Buisness Media, 2004, ISBN: 0-387-22575-7.
5. D.K. Arrowsmithv and C.M.Place, "An Introduction to Dynamical systems", Cambridge Univ.Press (1990).
6. C.S. Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", 1st Edn., Idea Group Publishing, Taiwan, ROC, ISBN: 10: 1591401925, pp: 350, 2005..
7. Fan Tie-sheng, Xue Jian-sheng, Xuan Wei-hong, Qu Da-peng, "OFDM Information Hiding Method by Preposition Embedded QIM", CIMCA 2008, IAWTIC 2008 and ISE 2008.
8. Anamitra Makur, S. SethuSelvi, "Variable dimension vector quantization based image watermarking", Signal Processing 81 (2001) 889-893.
9. Hsien-Chu Wu, Chin-Chen Chang, "A Novel Digital Image Watermarking Scheme based on The Vector Quantization Technique", Computers & Security (2005) 24, 460-471.
10. Hideki Noda, MichiharuNiimi and Eiji Kawaguchi, "High-Performance JPEG Steganography using Quantization Index Modulation in DCT Domain, , Pattern Recognition Letters 27 (2006) 455–461.
11. A. Ouled Zaid, A. Makhloufi, A. Bouallegue and C. Olivier, "Improved QIM-based Watermarking Integrated to JPEG2000 Coding Scheme", SIViP (2009) 3:197–207, DOI 10.1007/s11760-008-0094-z.
12. Chin-Chen Chang and Wen-Chuan Wu, "Reversible Quantization-Index Modulation Using Neighboring Correlation", IWDW 2007, LNCS 5041, pp. 222–232, 2008.
13. Mahalingam Ramkumar, Ali N. Akansu and A Aydan Alatan, "A Robust Data Hiding Scheme for Images using DFT", In Proceedings of ICIP (2)'1999. pp. 211-215.
14. Jinhua Liu, Kun She, and William Zhu, "Using Wavelets and Independent Component Analysis for Quantization Index Modulation Watermarking", Springer-LNCS 5589, pp. 555–562, 2009.
15. Xianfeng Zhao, Bingbing Xia, and Yi Deng, "Strengthening QIM-based Watermarking by Non-uniform Discrete Cosine Transform", LNCS 5284,pp.309–324,2008

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication