ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 45-48 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain

K.Babyrani , T.Geetamma
[1]GMRIT, India, kundiri_babyrani@yahoo.co.in
[2]GMRIT, India, tgeetamma@yahoo.co.in

Abstract : Attaining robustness, imperceptibility and high capacity are of great rank in digital watermarking. In this paper a new watermarking technique is introduced based on the ideologies of informed coding and informed embedding. A hidden markov model (HMM) in the wavelet domain is developed to convert image into vector tree. An optimal embedding strength vector is obtained by using the Viterbi algorithm. The hidden markov model avoids the problem of unobtainability of exact embedding strength in the receiver due to informed embedding. Because of HMM based detector at the receiver the performance of watermarking is degraded so Taylor series approximated locally optimum test (TLOT) detector is developed to improve the detection performance in the extraction algorithm. The proposed robust watermarking algorithm has high sturdiness against common attacks in signal processing and shows a comparable performance in the state of the art scheme with a greatly reduced arithmetic complexity.

Key words : informed coding, informed embedding, hidden markov model(HMM),wavelet, TLOT detector.

INTRODUCTION

Digital watermarking developed as a solution for protecting the multimedia data .Digital Watermarking is the process of hiding or inserting an invisible signal (data) to the given signal. The main objective of watermarking is robust watermarking ,which aims at attaining sturdiness, imperceptibility and capacity at once [2],[3][6].these three objectives ,however, are opposing to each other, and thus a good design is required to attain an appropriate tradeoff between them. Digital watermarking methods are closely related to the problem of communication with side information at the transmitter.

Digital Image watermarking is a method to hide the secret image (watermark image) into cover image resulting watermarked image [4]. Watermark image has to sustain against several attacks on watermarked image as well as it can be imprinted on the cover image either by visible or invisible, it may be Binary, Gray or color image .Size of the watermark image that can be embedded depends on the algorithm used for watermarking and also it provides copyright protection of image data by hiding appropriate information in the original image.

In general, digital watermarking can be categorized into two classes depending on the domain of watermark inserting i.e., the spatial and transform domain. Spatial domain methods are less composite and not robust against various attacks as no transform is used in them. Transform domain methods are robust as compared to spatial domain methods.

Types of Watermarks:

- Visible watermark
- Invisible watermark
  a) Robust watermark
  b) Fragile watermark

Visible:
An image (watermark) that is overlaid on the primary (cover) image, which is visible in the watermarked image

Invisible:
An image (watermark) which is overlaid on the primary (cover) image, which is invisible, but which can be detected algorithmically

Robust watermark:
This watermark has the ability to withstand to various attacks on watermarked image thus providing copyright protection.

Fragile watermark:
This watermark is mainly used for detecting modified data of the watermarked image. This watermark gets degraded even for a slight modification of data in the watermarked image.

Requirements of Digital Image Watermarking:
Imperceptibility
Robustness
Inseparability
Security
Capacity

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 45-48 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Imperceptibility: The embedded watermarks are imperceptible both perceptually as well as spastically and do not alter the aesthetics of the multimedia content that is watermarked. The watermarks do not create visible artifacts in still images, alter the bit rate of video or introduce audible frequencies in audio signals.

Robustness: Depending on the application, the digital watermarking technique can support different levels of robustness against changes made to the watermarked content. If digital watermarking is used for ownership identification, then the watermark has to be robust against any modifications. The watermarks should not get degraded or destroyed as a result of unintentional or malicious signal and geometric distortions like analog-to-digital conversion, digital-to-analog conversion, cropping, resampling, rotation, dithering, quantization, scaling and compression of the content. On the other hand, if digital watermarking is used for content authentication, the watermarks should be fragile, i.e. the watermarks should get destroyed whenever the content is modified so that any modification to content can be detected.

Inseparability: After the digital content is embedded with watermark, separating the content from the watermark to retrieve the original content is not possible.

Security: The digital watermarking techniques prevent unauthorized users from detecting and modifying the watermark embedded in cover signal. Watermark keys ensure that only authorized users are able to detect/modify the watermark.

Capacity: Capacity is one of the most important parameters in image watermarking .Determining the capacity of watermark in a digital image means finding how much information can be hidden in images without perceptible distortion, while maintaining watermark robustness against usual signal processing manipulation and attacks.

In this method, developing an algorithm for inserting the robust image watermarks with large data payloads using informed embedding and informed coding techniques by using hidden markov model (HMM) in the wavelet domain (HMM-WD) is introduced. This is for the application of copyright protection. Discrete wavelets transform are used to get a robust image watermark. But in the case of WD-HMM [5] sturdiness, invisibility and capacity are achieved at a time. TLOT Detector is used in the extraction algorithm to remove the message from the watermarked image. Taylor series approximation locally optimum test (TLOT) detector is established to increase the detection performance.

DISCRETE WAVELET TRANSFORM

The wavelet transform has emerged as an exciting new tool for statistical signal and image processing. It provides a natural setting for many applications involving real-world signals, including estimation, detection, compression, classification and filtering. Discrete wavelet transform (DWT) uses filter banks to perform the wavelet analysis. The discrete wavelet transform decomposes the signal into wavelet coefficients from which the original signal can be reconstructed again the wavelet coefficients represent the signal in various frequency bands. Discrete wavelets transforms are used to obtain only a robust image watermark, but in case of WD-HMM the robustness, invisibility and capacity are achieved at once.

WD-HMM:

The hidden markov chain model links the state variables horizontally within each scale the hidden markov tree model links the state variables vertically through scale ,then denote to these models jointly called as wavelet domain HMMs. [5]

PROPOSED METHOD

This introduced method contains three sections i.e., The Transmitter, the receiver and the Block diagram of watermark embedding and the watermark extraction algorithm. Transmitter(as shown in fig 1) acts as a watermark embedding algorithm and the receiver acts as a watermark extraction algorithm or watermark detection algorithm.

Transmitter

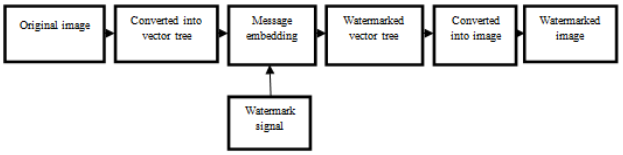

Fig.1. watermark embedding algorithm

Transmitter acts as a watermark embedding algorithm. It converts original image into vector tree by using wavelet transform. This converted vector tree is given to the message embedding as a one input and other input is watermark signal the output of the message embedding is a watermarked vector tree. Each two level vector tree called 'T' contains five sub vectors or vector nodes. Hence vector tree has 15 nodes totally. This 15 node vector tree will assist as the basic unit for watermarking .It is used as the carrier for the watermark message. This watermarked vector tree is further converted into image i.e. watermarked image as shown in the figure 2.

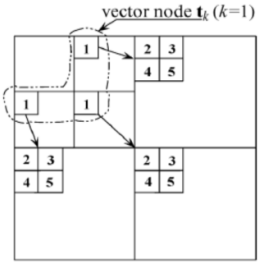

Fig.2. two-level wavelet pyramid for watermarking, where coefficients with the same number k (k=1…..5) are grouped into one vector node t_k.

$$\boldsymbol{H}_j = \begin{pmatrix} p_j^{1\to1} & p_j^{1\to2} \\ p_j^{2\to1} & p_j^{2\to2} \end{pmatrix}, j = 2,3,\ldots,J$$

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 45-48 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

The coefficients at the same scale(j) and location (k) at different subbands are grouped into one vector node. which is denoted as $t_{j,k}=(t^1_{j,k}, t^2_{j,k}, t^3_{j,k})$. where $t^1_{j,k}$, $t^2_{j,k}$ and $t^3_{j,k}$

Denote the wavelet coefficients at horizontal (H),vertical(v),and diagonal(D) orientations, respectively.

Each two level vector tree called 'T' contains five subvectors or vector nodes. hence vector tree has 15 nodes totally.
This 15 node vector tree will serve as the basic unit for watermarking.
It is used as the carrier for the watermark message.

Receiver

Fig.3. watermark extraction or detection algorithm

Receiver (as shown in fig 3)acts like watermark extraction algorithm, it converts the watermarked image into vector tree that is given to the message extraction algorithm input. The output of the message extraction algorithm is watermark signal.

Watermark Embedding and Watermark Extraction:

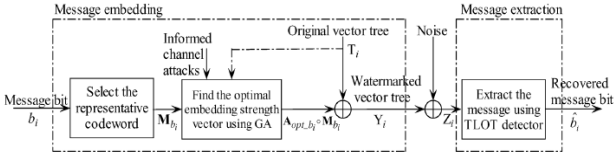

Fig.4. Block diagram of watermark embedding and watermark extraction.

The HMM-based informed coding and embedding watermarks algorithm, which include the message embedding and extraction processes are shown in figure 4. For each vector tree T_i, the embedding process consists of two stages, i.e., choosing the representative codeword M_{bi} according to the input message bit b_i (b_i=0,1) and utilizing the viterbi algorithm VA- based informed coding and embedding to find the optimal embedding strength vector $A_{opt\_b_i}$ for M_{bi}.[7]

Informed coding: The source of informed coding is to perform an intelligent message codification depending on the cover work.

Informed embedding: The main objectives of this technique are to adapt every watermark to the cover work maintaining a relationship between the watermarks desired robustness and the distortion effect produced in the image. In informed embedding, the chosen code word is tailored according to both the host signal and the constraints of robustness and distortion. The extraction process consists the TLOT detector it is used to recover the message. TLOT Detector (Taylor series approximation locally optimum test) Taylor series approximation locally optimum test detector is established to increase the detection performance.

Message Embedding Process:

Let the host signal I(x,y)be an image of size L_1xL_2.Suppose that the to-be-embedded message **b** consists of random bits. The embedding process of the proposed HMM-based informed coding and embedding watermarking can be described as follows.

1. The host signal is first decomposed using with a three-level wavelet pyramid, and use the coarsest two levels to construct vector tree as shown in fig.2
2. To attain good robustness, insert one bit into one vector tree, which in turn requires producing the message **b** of random bits .permute **b** with the secret key **KEY** so as to enhance the confidentiality. Allocate one permuted bit b_i (b_i=0, 1) to each vector tree $\mathbf{T}_i$.
3. Associate the prearranged message bit b_i to its representative codeword $\mathbf{M}_{bi}$.
4. Determine the optimal strength vector $\mathbf{A}_{opt\_bi}$ for M_{bi}. Through informed coding and embedding, which is formulated as a GA-based optimization problem and embed ($\mathbf{A}_{opt\_bi} \bigcirc \mathbf{M}_{bi}$) into $\mathbf{T}_i$ via the rule $\mathbf{Y}_i=\mathbf{T}_i+\mathbf{A}_{opt\_bi} \bigcirc \mathbf{M}_{bi}$.
5. Once finishing inserting all message bits into their corresponding vector trees and perform the inverse wavelet transformation to attain the watermarked image $\mathbf{I}^w(x, y)$.

Message Extraction Process:

For a specified vector tree $\mathbf{T}_i$, the two embedding strength vectors E_0 and E_1 (corresponding to b_i=0 and 1,respectively) are constrained so that the resulting codewords ($E_0 \bigcirc M_0$) and ($E \bigcirc M_1$) are located in the neighborhood of M_0 and M_1,which can be efficiently detected by the TLOT detector. Upon receiving the possibly attacked watermarked image $\mathbf{I}^p(x,y)$,the TLOT detector is employed to recover the message from $\mathbf{I}^p(x,y)$ which is outlined as follows.

1. Decompose the watermarked image $\mathbf{I}^p(x,y)$ into a three level wavelet pyramid and then create the vector trees using the coarsest two levels.
2. for each vector tree ,employ the TLOT detector to find a codeword with the maximum TLOT value, called $M_{bi}^p \varepsilon\{M0,M_1\}(b_i^r=0,1)$.
3. Take the corresponding coset index (0 or 1) of $\mathbf{M}_{bi}$ as the extracted message bit $b^p_i \varepsilon\{0,1\}$.
4. After processing all vector trees ,reorder the extracted bit sequence with the key KEY to recover the message sequence b_r.

Simulation Results:

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 45-48 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

HOST IMAGE:

Fig.5. original image of lena (size 512x512).

WATERMARK SIGNAL:

Fig.6. watermark signal

WATERMARKED IMAGE:

Fig.7. watermarked image of lena

THREE LEVEL DWT:

Fig.8.after applying 3-level DWT.

RECOVERD WATERMARK IMAGE:

Fig.9.extracted watermark signal.

EXPERMENTAL RESULT

In this section measure the watermarked images in terms of peak signal- to -noise ratio (PSNR) and correlation coefficients.as shown in table 1. This method Evaluate the performance of the introduced HMM-based informed coding and embedding algorithm.

Table 1: Attack class of watermarked image and recoverd watermark.

Attack class	Watermarked Image	Recoverd Watermark
PSNR	56.84 dB	58.64 dB
Correlation coefficient	0.67	0.78

CONCLUSION

Informed coding decreases the fidelity of the watermarking process and,on the other hand informed embedding ensures a specified robustness only these two approaches provide satisfactory results.Attaining high robustness ,invisibility and capacity by using HMM –based informed coding and embedding.The greatest important properties of image watermarking systems are its robustness, invisibility ,data capacity.

introduced an HMM based DWT algorithm this watermarking system exhibits good robustness ,invisibility, and high capacity at a time.when compare with DWT algorithm

REFERENCES

[1]. Matt Miller,Gwenael J.Doerr,and Ingemar J.Cox, Senior Member,IEEE "Applying informed coding and embedding to design a Robust High-Capacity Watermark"IEEE Transactions on image processing,vol.13,no.6, june 2004.
[2]. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. San Mateo, CA: Morgan Kaufmann, 2001.
[3]. P.Moulin and J.A.O'Sullivan, "information-theoretic analysis of information hiding," in Proc.IEEE Int. Symp. Inform.Theory,Jun.2000,p. 19.
[4]. P.Moulin and R.Kotter, "Data-hiding codes," proc.IEEE, vol 93,no.12,pp.2083-2016,Dec.2005.
[5].M.S.Crouse,R.D.Nowak, and R.G.Baraniuk, "Wavelet-based statistical signal processing using hidden Markov models," IEEE Trans.Signal process.,vol.46,no.4,pp.886-902,Apr.1998.
[6].I.J.Cox, M.L.Miller,and A.L.McKellips, "Watermarking as communications with side information," Proc.IEEE,vol.87,no.7,pp.1127-1141,Jul.1999.
[7]. A.J Viterbi, CDMA:Principles of spread spectum communications:Reading.MA:Addison-Wesley,1995.