Indian J. Innovations Dev., Vol. 1, No. 6 (June 2012) ISSN 2277 - 5390

Optimum detecting of contour let-based image watermarks in a noisy environment

Vidhyalakshmi M*, Vennila G

Department of Computer Science and Engineering, Jayaram College of Engineering and Technology, Trichy, Tamil Nadu, India

****Corresponding author:*** Department of Computer Science and Engineering, Jayaram College of Engineering and Technology, Trichy, Tamil Nadu, India.

Abstract

The objective of this paper is to analyze the unsteady magneto hydrodynamic flow of a viscous incompressible fluid past an infinite hot vertical porous plate in presence of constant suction and periodic variation of plate temperature. The governing equations of the flow field are solved employing multiparameter perturbation technique assuming Eckert number as perturbation parameter. The effects of magnetic parameter M, Grashof number for heat transfer Gr, Eckert number Ec, Prandtl number Pr, frequency parameter ω, etc. on velocity, temperature, skin friction and heat flux are discussed with the help of figures and tables. It is observed that a growing magnetic parameter enhances the velocity of the flow field near the plate and there after the effect reverses due to the magnetic pull of the Lorentz force on the flow field. The Grashof number/permeability parameter/Eckert number has an accelerating effect on the velocity of the flow field. A growing Prandtl number / Reynolds number has a retarding effect on the temperature of the flow field at all points. The permeability parameter enhances the skin friction and decreases the magnitude of heat flux at the wall. On the other hand, the magnetic parameter enhances the skin friction as well as the magnitude of heat flux at the wall.

Keywords: Contourlet transform; Maximum likelihood detector; Multiplicative image watermarking.

Abbreviations: GGD - General Gaussian distribution, ML - Maximum Likelihood, AWGN- Additive White Gaussian Noise, DCT - Discrete Cosine Transform, HVS- Human Visual System, DFT- Discrete Fourier Transform, CT- Contour let transform.

Introduction

Information hiding is an emerging research area which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and data embedding. In particular, watermarking is now a major activity in audio, image, and video processing and standardization efforts for JPEG-2000, MPEG-4, and digital video disks are underway. Commercial products are already being developed.

In our generic information-hiding problem, a message is to be embedded in a host data set, and the resulting data set may be subject to data processing operations (attacks) that attempt to remove any trace of form. The information- hiding system should satisfy two basic requirements. The first requirement is usually referred to as *transparency* or *unobtrusiveness*: the data set should be similar to, according to a suitable distortion measure. The second requirement is referred to as *robustness*: the hidden message should survive the application of any data processing technique (within a certain class). Often there is a limit on the amount of distortion that an attacker is willing to introduce.

In watermarking applications, the message contains information such as owner identification and a digital time stamp. The goal here is usually copyright protection. The message itself is not secret, but it is desired that it permanently resides within the host data set. Similar requirements exist for systems that embed data (such as object identification, text, or audio), in image and video databases. Such applications are commonly referred to as data hiding or data embedding. Closely related to watermarking is the fingerprinting, or traitor tracing, problem, where in addition to copyright information, the owner of the data set embeds a serial number, or fingerprint, that uniquely identifies the user of the dataset and makes it possible to trace any unauthorized use of the data set back to the user. This application is particularly challenging as it opens up the possibility of collusion between different users to remove these fingerprints. A different type of application is the embedding of data such as multi-lingual soundtracks in pay-per-view television programs. Here, the message is secret in the sense that it should not be decipherable by unauthorized decoders.

This paper introduces the digital watermark must have special features to guarantee desired functionalities. Perceptual transparency, data rate, and robustness against attacks are three major requirements of any watermarking system. There is a trade-off among these requirements which has been investigated in (Moulin and Sullivan, 2003) and (Maor and Merhav, 2005) from an information-theoretic perspective. However, depending on the application, the importance of these features varies. For example, for secret communication systems, the robustness against noise and data rate is the most important feature, while for data authentication; imperceptibility and robustness against different processing attacks are the most significant ones.

The increase of the power of watermark causes more resistance against attacks. This point leads designers to choose the energy of the watermark to be dependent on the still image powers. In the attempt to match the characteristics of the watermark to those of the image features, larger image information contents bear greater watermark. In other words, the power of the watermark is proportional to the corresponding image feature samples. The simplest way to implement this principle is by means of multiplicative watermarking. In order to employ the Human Visual System (HVS) properties, multiplicative watermarking is often used in the transform domain. The transforms usually selected for digital watermarking are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) (Hsu and Wu, 1998) (Akhaee *et al*., 2009) which concentrate the energy of the host signal in a fewer components. It has been proven that the kernel of DWT is well suited for representing one-dimensional discontinuities. However, when the dimension increases, wavelets fail to represent singularities.

The main advantage of contour let transform over other directional representations is that it allows different number of directions at each scale while achieving nearly critical sampling. Besides, it employs iterated filter banks, which makes it computationally efficient. By utilizing the performance of the contour let transform in capturing directional information of image edges, some watermarking algorithms have been proposed. In the additive watermarking methods are proposed, while references investigate the multiplicative watermarking approaches.

In this paper, in order to achieve higher robustness against AWGN and JPEG compression attacks, the multiplicative watermarking approach in the contour let transform domain is used. We introduce a new multiplicative watermarking scheme to match the watermark message to the contour let coefficients in an optimum way. The contour let coefficients are multiplied by two special functions depending on the value of the watermark bits. These functions are optimized for the highest robustness against AWGN and JPEG attack. For data extraction, similar to the ML detector has been used utilizing GGD property of the contour let coefficients. To this aim, the density function of the noisy contour let coefficients is analytically computed. In order to decrease the complexity of the receiver, the distribution of these coefficients is approximated with a suitable function. Under this estimation, the optimum threshold of the proposed multiplicative watermarking method is evaluated. We also extend the proposed method to a blind technique which does not need side information.

Information hiding

Information hiding can be thought of as a game between two co-operative players (the information hider and the decoder) and an opponent (the attacker). The first party tries to maximize a payoff function, and the opponent tries to minimize it. Then the information available to each party critically determines the value of the game. If the players choose their actions in a given order, then a conservative approach for the first player is to assume that the second player will find out what the first player's action is.

An operational definition of information - hiding capacity. We show that memory less attacks are optimal within a certain class of attack channels with memory that attacks are memory less and show that capacity is the value of a mutual-information game between the information hider and the attacker. In order to maximize the payoff, the information hider optimally designs

- Covert Channel
- Attack Channel

Hiding Capacity

Four key differences between our setup and *Gel'fand and Pinsker's are*

- The presence of distortion constraints;
- The availability of side information at the encoder and the decoder;
- The fact that the encoder does not know the attack channel and
- The unavailability of to the attacker.

Wavelet transform

Wavelet packets naturally come to mind as a potential dentition of an *ortho* normal basis satisfying these localization properties. They also come with fast algorithms. The wavelet packet tree, dining the partitioning of the frequency axis in 1D, can be chosen to have depth (Demanet and Ying, 2005). However, there is a well-documented problem associated with standard wavelet packets, namely that the sense in which they satisfy frequency localization is rather weak. It is an unavoidable feature of the filter bank architecture that the uncertainty (product of time and frequency deviations) increases with the frequency, instead of remaining close to the Heisenberg bound. For references, for precise estimates of the wavelet packet curse as a result, in our context, we cannot hope to satisfy the wave atom definition using basis functions which come from a wavelet packet analysis.

Here four problems are occurred

- oscillation
- shift variance
- aliasing
- lack of directionality

Curve let transform

Curve let transform is defined to represent two dimensional discontinuities more efficiently, with less error in a fixed term approximation. However, since curve let transform has been introduced in continuous domain; it does not have acceptable performance in critical discrete applications. As an improvement on the curve let transform, Contour let Transform (CT) is proposed by using Pyramidal Directional Filter Bank (PDFB). The main advantage of contour let transform over other directional representations is that it allows different number of directions at each scale while achieving nearly critical sampling. Besides, it employs iterated filter banks, which makes it computationally efficient. By utilizing the performance of the contour let transform in capturing directional information of image edges, some watermarking algorithms have been proposed. In the additive watermarking methods are proposed, while references investigate the multiplicative watermarking approaches.

Contour let transform

Contour let Transform (CT) is proposed by Do *et al.* (2005) using Pyramidal Directional Filter Bank (PDFB). The main advantage of contour let transform over other directional representations is that it allows different number of directions at each scale while achieving nearly critical sampling (Do *et al.*, 2005). Besides, it employs iterated filter banks, which makes it computationally efficient. By utilizing the performance of the contour let transform in capturing directional information of image edges, some watermarking algorithms have been proposed so far. In (Jayalakshmi *et al.*, 2007) the additive watermarking methods are proposed, while references investigate the multiplicative watermarking approaches.

For piecewise continuous 1-D signals, wavelets have been established as a right tool in generating efficient representation. However, natural images are not simply stacks of 1-D piecewise smooth scan-lines, but they have many discontinuity points along smooth curves and contours. Thus, separable wavelets cannot capture directional information in two dimensions. To overcome this shortcoming, many directional image representations have been proposed. Implementations of idea for combining sub band decomposition with a directional transform.

Watermark embedding

The watermarking algorithm (Fig.1) is commonly achieved by exploiting the weaknesses of the HVS. As demonstrated in HVS, the human eye is less sensitive to high entropy blocks instead of smooth ones as there are usually stronger edges in the high entropy blocks. For this purpose, we select blocks with the highest entropy in the whole image for the watermarking purpose. We then apply the contour let transform to each selected block. Calculating the energy of the coefficients in each directional sub band of the finest scale, we choose the directional sub band with the highest energy for embedding purpose. This way, we hide the code in the most significant direction of each block.

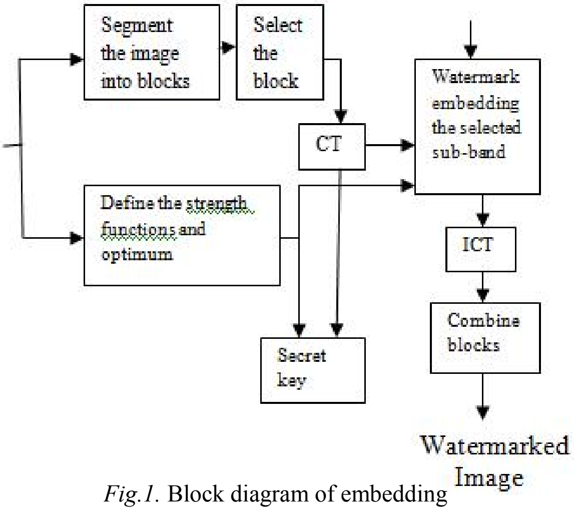
Segment the image into blocks
Select the block
CT
Watermark embedding the selected sub-band
Define the strength functions and optimum
ICT
Combine blocks
Secret key
Watermarked Image

Fig.1. Block diagram of embedding

single bit of “0” or “1” in each block by manipulating the coefficients in the most energetic directional sub band based on the following strategy:

$$\omega_i = \begin{cases} xi.\,f1(xi), & for\ embedding\ 1 \\ xi.\,f0(xi), & for\ embedding\ 0 \end{cases} \quad (1)$$

where and are strength functions. Applying the inverse contour let transform, we reconstruct the watermarked block. Repositioning each block in its position in the image, we create the watermarked image. The block positions and the GGD parameters (and) should be sent along with the watermarked image.

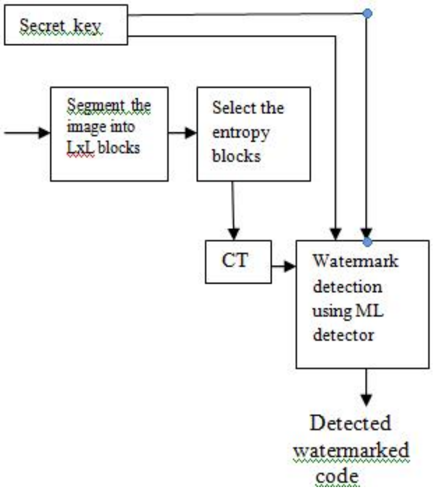
Secret key
Segment the image into LxL blocks
Select the entropy blocks
CT
Watermark detection using ML detector
Detected watermarked code

Fig .2. Block diagram of detecting

Watermark detecting

For detecting the watermark data in each block, we suggest a detection scheme based on an optimum detector (Fig.2). Suppose that represents the contour let coefficients of the most energetic directional sub band of a specific block. We assume these coefficients to be independently and identically distributed (i.i.d.). Besides, we approximate the distribution of the watermarked coefficients attacked by AWGN.

In order to have ML decision, we must have

$$P(y1, y2, \ldots, ym|\,1)\frac{\leq 0}{>1}P(y1, y2, \ldots, ym|\,0)$$

Where the left term is the distribution of the co-efficient in a specific block with coefficients for

"1" embedding and the right term is the same distribution for "0" embedding.

Parameter optimization

The effect of the strength function on the visibility using the image quality index suggested in (Wang and Bovik, 2009). In this quality assessment method, any image distortion is modeled as a combination of three factors considering the properties of the HVS:

1) Loss of correlation,
2) Luminance distortion, and
3) Contrast distortion.

This image quality index outperforms traditional quality assessment methods such as MSE due to its conformity to HVS and subjective tests. The strength functions and have critical role on the performance of the watermarking scheme. These functions can affect two factors in the watermarked image: visibility and robustness. Since, can be calculated from through (Demanet and Ying, 2007) we only consider the effect of. First, larger values of can cause more distortions in the image due to the watermark. On the other hand, larger values of increase the robustness of the watermarked image against various attacks. Therefore, there is a trade-off between visibility and robustness. We utilize a multi-objective optimization technique to select an appropriate strength functions ensuring imperceptibility with acceptable robustness.

Experimental setup

This section describes the experiments conducted to natural images. For this study, we use five natural images (*Baboon*, *Barbara*, *Map*, *Bridge*, and *Couple*) of size 512 512. The original test images and their watermarked version using the proposed method with 16 16 block size and 128 bits message length as well as the five times scaled of the absolute difference between the watermarked and the original image . As we can see, the watermark invisibility is satisfied. The mean Peak-Signal-to-Noise-Ratio (PSNR) between the original and the watermarked images are 39.53, 36.63, 39.87, 42.40, and 42.48 dB, respectively.

For the proposed semi-blind approach, a typical side information bit budget needed for an image of size 512 512 and assuming 16 16 block size and 128-bit message length is as follows:
i) block positions:1 bit/block = $(512/16)^2$ =1024 bits (we send "1" if a block is among the high entropy blocks and "0" otherwise);1024 bits
ii) 4-bit words for the shape parameter and 8 bit words for the ML parameter: 12.128 =1536 bits;
iii) a3: 8 bits.

Thus, the raw side information necessitates 2568 bits/image. The block positions, however, can be compressed to near 512 bits on the average using Arithmetic coding as a lossless coding. Other block parameters also can be reduced with lossy coding to near 1024 bits using Vector Quantization (VQ) with negligible loss in the performance. Thus, in total the side information is reduced to near 1.5 Kbits on the average per image.

- Capacity
- Performance under attack
- Salt & Pepper Noise Attack
- Rotation Attack.

Conclusion

This paper introduced a robust multiplicative image watermarking technique in the contour let transform domain. The proposed algorithm is presented in both semi-blind and blind versions. Since the contour let transform concentrates the image energy in the limited number of edge coefficients, using multiplicative approach in this domain yields high robustness accompanied by great transparency. To have better control on both imperceptibility and robustness, the strength functions are selected optimally by multi-objective optimization approach. We model the distribution of contour let coefficients by GGD. Then, the distribution of watermarked noisy coefficients is calculated analytically. Using ML decision rule, the optimum detector has been proposed. Experimental results over several images confirm the excellent resistance against common attacks in the semi-blind version. In the blind version the proposed method performs recently proposed technique

AWGN and rotation attacks, while it has competitive results in JPEG attacks.

References

1. Akhaee MA, Sahraeian SME, Sankur B and Marvasti F (2009) Robust scaling-based image water marking using maximum-likelihood decoder with optimum strength factor. *IEEE Trans. Multimedia*. 11(5), 822–833.

2. Demanet L and Ying L (2007) Wave atoms and sparsity of oscillatory patterns. *Appl. Comput. Harmon. Anal*, 23, 368.

3. Do MN and Vetterli M (2005) The contour let transform: An efficient directional multi resolution image representation. *IEEE Trans. Image Process.* 14(12), 2091–2106.

4. Hsu CT and Wu JL (1998) Multiresolution water marking for digital images. *IEEE Trans. Circuit Syst.* 45(8) 1097–1101.

5. Jayalakshmi M, Merchant SN, and Desai UB (2006) Digital watermarking in contour let domain. *In Proc. 18th Int. Conf. Pattern Recognition*. 3, 861–864.

6. Maor A and Merhav N (2005) On joint information embedding and lossy compression in the presence of a stationary memoriless attack v channel. *IEEE Trans. Inf. Theory*, 51(9), 3166–3175.

7. Moulin P and O'Sullivan JA (2003) Information-theoretic analysis of information hiding. *IEEE Trans. Inf. Theory*. 49(3), 563–593.

8. Wang Z and Bovik AC (2004) Image quality assessment: From error visibility to structural similarity, *IEEE Trans. Image Process*. 13(4), 600–612.