International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:3, 2008

Distortion Estimation in Digital Image Watermarking using Genetic Programming

Labiba Gilani, Asifullah Khan, and Anwar M. Mirza

Abstract**—**This paper introduces a technique of distortion estimation in image watermarking using Genetic Programming (GP). The distortion is estimated by considering the problem of obtaining a distorted watermarked signal from the original watermarked signal as a function regression problem. This function regression problem is solved using GP, where the original watermarked signal is considered as an independent variable. GP-based distortion estimation scheme is checked for Gaussian attack and Jpeg compression attack. We have used Gaussian attacks of different strengths by changing the standard deviation. JPEG compression attack is also varied by adding various distortions. Experimental results demonstrate that the proposed technique is able to detect the watermark even in the case of strong distortions and is more robust against attacks.

Keywords**—**Blind Watermarking, Genetic Programming (GP), Fitness Function, Discrete Cosine Transform (DCT).

I. Introduction

DIGITAL watermarking has become a more challenging field to find the solutions related to vast appearance of digital data. Although, there are many technologies like, cryptography, steganography and information hiding that could be effective against these problems, but equally attackers are also developing more and more intrinsic attacks. Intelligent and adaptive techniques are required in order to cope with distortions introduced by the attacks. A watermarked data can be attacked in many different ways. However, each application usually has to deal with a particular sequence of distortions. Several strategies have been implemented to make a watermark system reliable [3, 5, and 6]. Cox et al. [1] and Barni et al. [2] have also discussed in detail the types and levels of robustness that might be required for a particular watermarking application. They have discussed some of the attacks and their countermeasures.

Voloshynovsky et al [7] have performed optimal adaptive diversity watermarking with channel state estimation. They have considered watermarking as a communication problem with the side information provided at both the encoder and decoder end. However, side information at the decoder through private channel is not always desirable.

Khan et al [10] have proposed the idea of developing a GP based model applicable to any robust watermarking system. The proposed technique exploits the characteristics of Human Visual System. The developed model allows the maximum imperceptible alterations to a DCT matrix of cover image. Also, Khan et al in [8] have suggested the idea of structuring the watermark in accordance with an anticipated attack. This is done by spreading and fusing the watermark in such a way that it not only attains a superior tradeoff between the robustness and imperceptibility but also resists conceivable attacks. It utilizes cover image and conceivable attack information during watermark embedding. They consider perceptual shaping functions not only important to increase imperceptibility but also to structure the watermark in accordance to anticipated attack. They used information about Watson Perceptual Model, characteristics of HVS, and distortions introduced by attacks as independent variables and genetically search for application specific perceptual functions. In another paper [9], to make their proposed scheme more robust, they have proposed the idea to develop such a decoder that modifies itself according to a cover image and conceivable attack using Genetic Programming. Search space is exploited according to the types of dependencies of decoder on different factors.

One way to resist attack is to invert distortions at the decoding side. However, this usually is difficult to handle due to the matrix inversion problems. Therefore, in this work, our emphasis is on increasing robustness of a watermarking system by estimating the distortion occurred to a watermarked image. Rather inverting the distortions, we let the reference watermark suffer the same distortions using the estimated function before being correlated. Traditionally, at the receiving end, the performance of detection/decoding system decreases appreciably due to the distortions introduced by attacks. Our contributions in this regard are as such:

1. We consider distortion estimation as a function regression problem and use GP for its optimal solution.
2. We let the watermark signal at the decoding side suffer the estimated distortion before being correlated to the received cover signal.

The rest of the paper is organized as such: Section 2 is an introduction to Machine learning (ML) and Genetic

Labiba Gilani is with Faculty of Computer Sciences & Engineering, Ghulam Ishaq Khan (GIK) Institute of Engineering Science & Technology, Swabi, Pakistan (e-mail: labibagilani@hotmail.com).

Asifullah Khan is with Department of Information and Computer Sciences, Pakistan Institute of Engineering and Applied Sciences, Nilore, Islamabad, Pakistan (e-mail: asif@pieas.edu.pk).

Anwar M. Mirza is with Department of Computer Science, National University of Computer and Emerging Sciences, Islamabad, Pakistan (e-mail: anwar.m.mirza@nu.edu.pk).

Programming. It also describes the underlying watermarking scheme. Section 3 discusses our proposed methodology. Section 4 elaborates implementation details, while Section 5 presents results and discussion. The last section comprises conclusion and some future directions.

II. Related Theory

Machine learning refers to a system that can improve itself automatically through experience. This capability of learning from observation, experiences and other means, results in such a system that can continuously self improve itself and thereby provides more efficiency and accuracy. Eventually, the learning quality is evaluated by testing, how efficient the best solution of ML system can predict output from a test set. The test set must be generalized i.e. it should include other different examples than those for training set.

Genetic programming is a machine-learning model. It is a category of evolutionary algorithms, inspired by the mechanism of natural selection [11, 12, and 13]. It is most general and flexible all around and has already been applied to a wide variety of problems. It makes use of evolutionary algorithms to optimize a population of computer programs according to the fitness criteria specified by a program's ability to perform given computational task. It initially creates a large population of random programs and evaluates them. It retains the best individuals, while rests are deleted. In this way by selecting and scoring the individuals in each generation, solution space is refined generation by generation until it converges to optimal or near optimal solution.

In order to analyze the effectiveness of our proposed scheme, we use a simple and basic watermarking scheme [4]. To embed the watermark, first image is transformed into *DCT* domain, where zigzag scanning of the transformed image is performed to sort the coefficients suitable for watermark embedding. The first *L* coefficients are skipped and the watermark is inserted into next *G* coefficients. These new coefficients are then re-inserted into the zigzag scan. Watermarked image in spatial domain is then obtained by taking the inverse of modified DCT coefficients. In the detection process, Piva et al. [4] have used the inverse process for the recovered image. First, the *MxN DCT* coefficients matrix is computed. It is then re-ordered by the zigzag scan and *L+1* to *L+G* coefficients are selected. To determine the presence of a watermark, the correlation z is compared with the predefined threshold.

$$Z = \frac{1}{G}\hat{Y} \times S_o = \frac{1}{G}\sum_{i=1}^{G} \hat{Y}_{L+i} \times S_{0\,i} \qquad (1)$$

Where eq (1) is compared with the predefined threshold

III. Proposed Distortion Estimation Scheme

In this paper, we are developing distortion estimation function based on Genetic Programming. As in [4], the correlation computed is compared with the predefined threshold value. The best-evaluated distortion function is applied to original watermark and then the estimated correlation is compared with that of the correlation defined in [4]. The entire scenario can be considered as communication task with the watermark acting as signal, cover work acting as channel, whereas the attacks can be considered as noise. Our proposed scheme is supposed to detect the watermark from the corrupted image. In the sequel, we will represent in *DCT*-domain, the original cover image by X, the watermarked image by Y, and the received cover image by Z. The estimated watermarked signal is represented by $\hat{Z}$. The corresponding selected coefficients vectors are represented by a subscripts *v*, e.g. Z_v.

Our proposed methodology consists of two major modules; training and test modules. The functional diagram of our proposed methodology is shown in Fig. 1.

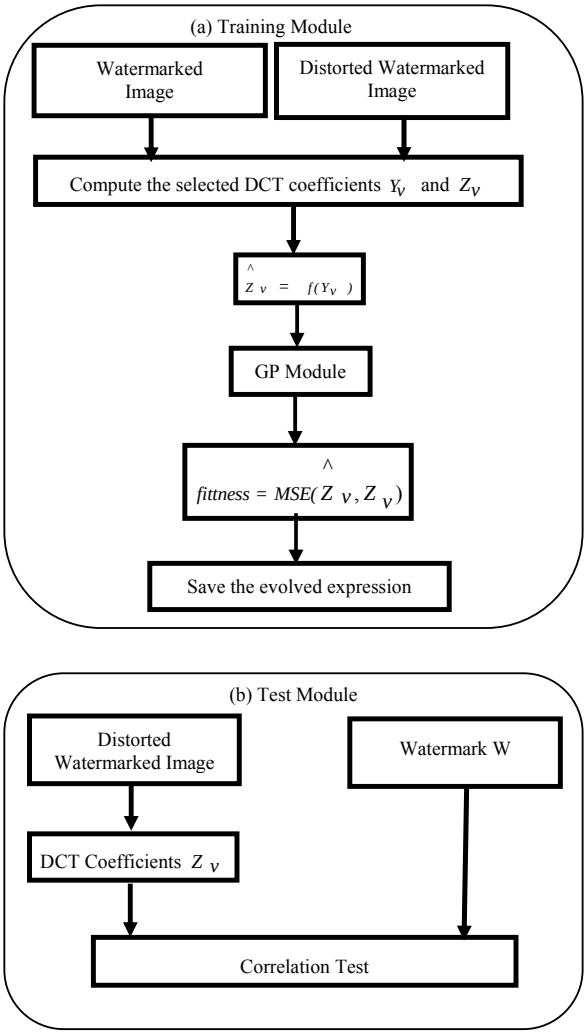


Fig. 1 Block Diagram of Proposed methodology

A. Training Module

In the current problem of estimating distortion function, we are passing the watermarked as well as distorted watermarked signals as input to our training module. The distortion function is estimated by considering the problem of obtaining a distorted signal from the original watermarked signal as a function regression problem. GP returns the best-estimated distortion function that is applied to original watermarked signal. All the attacks in our case are known attacks.

GP Function Set

The functions that we have used in our simulation are four binary floating arithmetic operators (+, -, *, and protected division), le (less than or equal to) and gt (greater than), SIN, COS, and Log.

GP Terminal Set

Other control parameters include the probabilities of performing the genetic operations, the maximum size for programs, and other particulars of the run. Combination of the two primitives, terminals and functions make up a GP tree, representing individual solution. Terminals in our case are independent variables, like original watermarked signal Y, μ_z, δ_z^2 and random constants.

GP Fitness Function

Fitness function in our case is Mean Squared Error (MSE) between the estimated watermarked signal and distorted watermarked signal.

$$MSE = \sum_{i=1}^{G} \frac{(Z_V^i - \hat{Z}_V^i)^2}{G} \quad (2)$$

Control Parameters

The control parameters are number of generations, population size, selection type, and termination criteria etc. We have used variable number of generations and population sizes for different simulations, whereas selection is Generational.

Initial Population

The initial population of a GP simulation is created by randomly generating trees. Ramped half and half strategy is used to creat initial population.

Termination Criterion

The GP simulation is ceased when the generation count reaches maximum number of generations, or when a program surpasses a threshold fitness level. If the termination criterion is accomplished, then continue. Otherwise, replace the existing population with the new population. Save the best individual in the population as the output of algorithm.

B. Test Module

In test module, we apply the best-evolved distortion estimation function to the original watermarked signal *M* hope to add the same channel distortion to the watermark as suffered by the cover image. We then, compare estimated correlation with that proposed by Piva et al [4]. We expect, as the results of section 5 shows, that the estimated correlation should be high.

IV. Implementation Details

We have used Matlab for our experimental studies. For the implementation of Genetic Programming, GP Lab toolbox of Matlab is used [20, 21]. The Parameter settings are shown in Table I. Lena image is used as a cover image in training. The GP based distortion estimation technique is checked for Gaussian attack and Jpeg compression attack with different strengths. Watermarking strength is kept constant at 0.2. We are using Gaussian attack of different strengths, as changing $\sigma = 15$ & 10. JPEG compression attack is also varied by adding 15% and 30% distortion. The expression obtained from training is tested on different images.

TABLE I
GP Parameters Setting

Objective	To evolve distortion estimation Fitness function
Function set	+, -, *, protected division, *SIN, COS,* and *LOG*
Terminal set	μ_z, δ_z^2 Original Watermark signal ***y***, e.t.c
Fitness	Mean Squared Error
Selection	Generational
Population Size	120
Initial max.Tree Depth	6
Initial Population	Ramped half and half
Operator prob. Type	Variable
Sampling	Tournament
Expected no. of offspring	Rank89
Survival mechanism	Keep best
Real max level	30
Termination	Generation 32

V. Results and Discussions

Two types of attacks are considered in order to analyze the potential of our GP-based technique for estimating distortion function; Gaussian noise attack, and JPEG compression attack. The experimental results show the correlation comparison of two schemes for Gaussian and Jpeg compression attacks with different strengths.

A. Performance Comparison against Gaussian Noise Attack

In the scenario given below, we have performed Gaussian attack on the watermarked image of Lena.

Fig. 2 Original gray scale Lena image

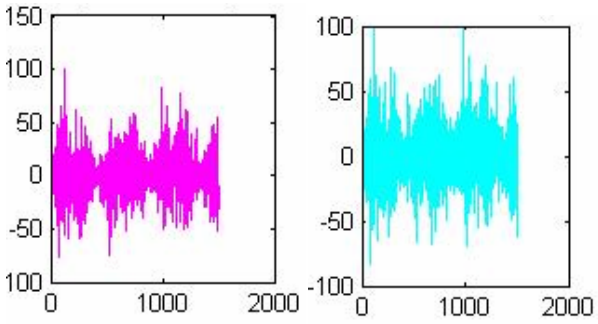
Fig. 3 Watermarked Gaussian attacked image

We have used Lena image of size 512x512 with 1500 selected number of training and test coefficients. Training data for the Gaussian attack is given in Table II.

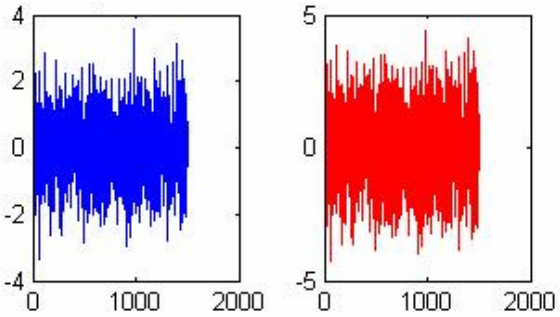
TABLE II
TRAINING DATA FOR GAUSSIAN ATTACK

Gen	Pop	σ	Correlation	Estimated Correlation
90	260	10	0.7383	1.1049
60	260	15	0.7507	1.0745

The expression and test of correlation results for the given expression are shown for other images in Table III given below to demonstrate the performance comparison of two techniques. It can be observed that GP-based distortion estimation scheme shows superior performance as compared to the one proposed in [4].



(a) Original WM cover work (b) received cover work



(c) Original WM Signal (d) Estimated WM signal

Fig. 4 Test case using Lena image

TABLE III
CORRELATION COMPARISON WITH Σ = 10 FOR DIFFERENT IMAGES

Images	Corr	Estm-Corr
Baboon	1.6570	2.4577
Boat	0.8333	1.2500
Couple	0.9151	1.3657
Trees	0.9628	1.4522
Pepper	0.6750	1.0013

Evolved expression in prefix form:

$+ (y_v , \sin (/ (y_v ,-(/ (0.60321, 0.35691), \mu_z))))$

Proposed GP based distortion estimation scheme could also be applied in general to signal processing applications, especially in communication and medical oriented applications.

Fig. 5 Original gray scale boat image

Fig. 6 Watermarked Gaussian attacked image

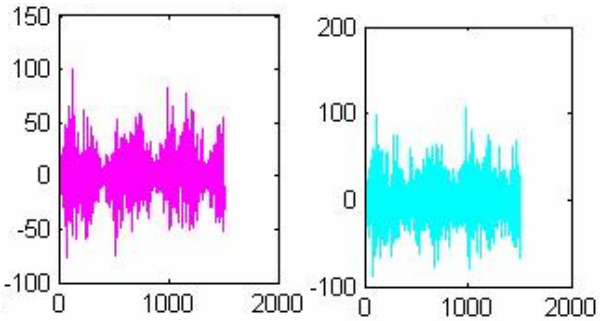
The above Figs. 5 and 6 show the original and watermarked attacked image after adding the Gaussian noise using σ =15. The approximate channel distortion estimated by GP is added to original watermark signal and the results of correlating distorted watermarked image with the distorted watermark are shown below in Table IV for the above image and other test images.

TABLE IV
CORRELATION COMPARISON WITH σ = 15 FOR DIFFERENT IMAGES

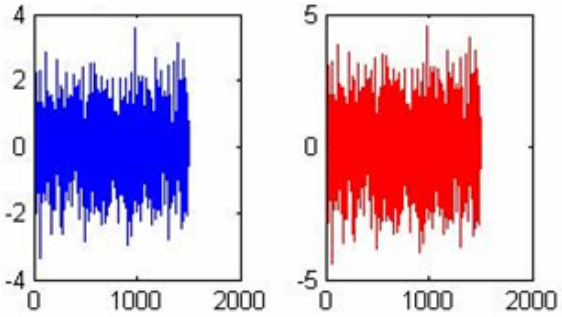
Images	Corr	Estm-Corr
Baboon	1.6673	2.3756
Boat	0.8442	1.2104
Couple	0.9294	1.3284
Trees	0.9750	1.4030
Pepper	0.6865	0.9771

Evolved expression in prefix form:

$+ (y_v , \sin (+ (-(*(0.48941, y_v), y_v) , y_v)))$



(a) Original WM cover work (b) received cover work



(c) Original WM signal (d) Estimated WM signal

Fig. 7 Test case using boat image

Although we have performed and validated our GP based distortion estimation idea on image watermarking however, it is equally well applicable in other watermarking applications, such as audio, video, 3D watermarking e.t.c. with similar reasons, besides watermarking.

B. Performance Comparison against JPEG Compression Attack

The proposed scheme is also tested for JPEG compression attack. It is equivalently showing superior performance than one proposed in [4]. The training data set using Lena image of size 512x512 with 3500-selected number of training and test coefficients using different Quality Factor (QF) for Jpeg compression attack is given in Table V.

TABLE V
TRAINING DATA FOR JPEG COMPRESSION ATTACK

Gen	Pop	QF	Correlation	Estimated Correlation
80	260	15	0.4470	0.5426
80	260	30	0.3394	0.4481

Fig. 8 Original gray scale Scale boat image

Fig. 9 Watermarked jpeg compressed image

The above figures show the original and jpeg compressed image using QF=15. Results and expressions of distortion estimation function using GP for Jpeg compression attack with QF=15 & 30 are given in Tables VI & VII shown below.

TABLE VI
CORRELATION COMPARISON WITH QF = 15 FOR DIFFERENT IMAGES

Images	Corr	Estm-Corr
Baboon	1.3888	1.6859
Boat	0.8518	1.0339
Couple	0.8131	0.9871
Trees	0.8730	1.0598
Pepper	0.5705	0.6925

Evolved expression in prefix form:

$+ (y_v ,*(/ (x\_m, \log (x\_V)), y_v))$

TABLE VII
CORRELATION COMPARISON WITH QF =30 FOR DIFFERENT IMAGES

Images	Corr	Estm-Corr
Baboon	1.3918	1.8224
Boat	0.7898	1.0321
Couple	0.7624	0.9970
Trees	0.8307	1.0941
Pepper	0.5394	0.7085

VI. CONCLUSIONS AND FUTURE DIRECTIONS

In this work, we have used Genetic Programming to develop efficient distortion estimation technique. The

proposed scheme has been tested against Gaussian and JPEG compression attacks with different strengths. We have estimated channel distortion using GP. In this way, at the decoding side we let the watermark signal suffer the estimated distortion before being correlated to receive cover signal. The experimental results have demonstrated that the GP based scheme has superior performance than the one proposed by Piva et al [4]. It can also be used for distortion estimation of signals in medical-oriented applications. It could also be applied in general to signal processing applications, especially in communication and medical oriented applications. The proposed scheme could also be applied to estimate distortion introduced by battery of attacks.

ACKNOWLEDGMENT

We acknowledge the support of Dr. Ajmal Bangash, Assistant Professor, GIK Institute during the course of this work.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and fundamentals, Morgan Kaufmann, San Francisco, 2002.
[2] M. Barni, and F. Bartolini, Watermarking systems engineering: Enabling digital assets security and other application, Marcel Dekker, Inc. New York, 2004.
[3] Kiryung Lee, Dong Sik Kim, Taejeong Kim, and Kyung Ae Moon, "Em estimation of scale factor for quantization-based audio watermarking," in Digital Watermarking,Second International Workshop,IWDW 2003, Seoul, Korea, Oct. 2003.
[4] A. Piva, M. Barni, F. Bartolini, V. Cappellini, DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image, Proc Int. Conf. Image Processing, vol. 1, Oct. 1997, pp. 520-523.
[5] J.C. Oostveen, A.A.C. Kalker, and M. Staring, "Adaptive quantize watermarking," in Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, California, USA, 2004, vol. 5306, pp. 37–39.
[6] Qiao Li, Ingemar J. Cox, Using perceptual models to improve fidelity and provide invariance to volumetric scaling for quantization index modulation watermarking, Campus Seminar Series, Departments of Computer Science and Electronic and Electrical Engineering, University College London Torrington Place, London, WC1E 7JE, England, Feb. 2005.
[7] Sviatoslav Voloshynovskiy, Frederic Deguillaume, Shelby Pereira and Thierry Pun, Optimal adaptive diversity watermarking with channel state estimation University of Geneva - CUI, 24 rue duGeneral Dufour, CH 1211, Geneva 4, Switzerland, 2002.
[8] A. Khan and Anwar M. Mirza, Genetic Perceptual Shaping: Utilizing Cover Image and Conceivable Attack Information Using Genetic Programming, accepted in International Journal of Information Fusion, Elsevier Science, 2005.
[9] Asifullah Khan, A Novel approach to decoding: Exploiting Anticipated Attack Information using Genetic Programming, International Journal of Knowledge-Based Intelligent Engineering Systems, 2006, (in press).
[10] A. Khan, Anwar M. Mirza and A. Majid, Intelligent Perceptual Shaping of a Digital Watermark: Exploiting Characteristics of Human Visual System, accepted in the International Journal of Knowledge-Based Intelligent Engineering Systems, 2005.
[11] W. Banzhaf, P. Nordin, R.E. Keller, and F.D. Francone, "Genetic Programming: An Introduction," Morgan Kaufmann Publishers, CA, 1998.
[12] S. Gustafon, "An Analysis of Diversity in Genetic Programming", PhD Thesis, University of Nottingham, UK, 2004.
[13] http://www.geneticprogramming.com.