Modeling and Analyzing Wavelet based Watermarking System using Game Theoretic Optimization Technique

Ms. Shweta[1], Mr. Akash Tayal[2] and Ms. Ankita Lathey[3]

[1]Department of Information Technology, Delhi Technological University, Delhi, India

[2]Department of Electronics and Communication, Indira Gandhi Institute of Technology, GGSIPU, Delhi, India

[3]FIITJEE Limited, Delhi, India

Abstract

This paper deals with establishing an economically viable and robust multilevel Game theoretic watermarking security system for the digital community; based on CPU time utilization with respect to channel capacity and system complexity. The coefficients of watermark are embedded into the host image at selected transformation level, which in turn extracted by inverse transformation at the decoder to develop the game matrix, which is iteratively searched for the optimized stable state for the system using permissible threshold. The rational thinking of maximizing the payoff of the watermarker (encoder) with respect to the attacker (noise) can be merged with the model deriving winning strategies to gain optimality. The data is rationally analyzed and tested to describe the behavior of the method for varying system parameter values and to gain performance optimization on different gray images with added Gaussian, salt and pepper, JPEG compression noises. Signal to noise ratio and correlation coefficients are used as criteria for testing the method.

Keywords: *Game theory, Rationality, Watermarking Wavelet Transform, Strategies.*

1. Introduction

In the recent years there has been a tremendous growth in the usage of digital media from desktops to laptops and to the hand-held devices [4], as a result of their ubiquitous accessibility. Future [5] will also include its colossal usage in the field of banking, data biding, auctions, military data transmission, etc [3]. This in turn demands high level of safeguard against the threat of intellectual property theft. One approach to address this problem is Digital watermarking technique, which establishes the "brand" ownership. Many watermarking techniques involve both spatial as well as transform domain (e.g., DCT, DFT, DWT, etc.). For a dynamic, technically sound and economically efficient watermarking system can be developed by using the basic ideas of classical Game Theory [6], as a complementary technique.

Game theory [9,10,11] is a tool for analyzing the interaction of decision makers with conflicting objectives. It typically assumes that all players seek to maximize their utility functions in a manner that is perfectly rational. Water marking is a typical game where two adversaries try to achieve two different, conflicting goals. Thus, we try to seek a critical balance between the two stake holders (players) i.e. watermarker and the attacker and will give a computationally optimized authentication system that will prevent bothering them from any kind of forgery.

In this dissertation we consider watermarking as a communication problem and design the solution to find the optimal way of embedding the hidden information in an image to overcome the distortion premised by various attacks using the multiresolution wavelet decomposition. Our proposed system will concern taking three main parameters: SNR, normalized coefficients, and CPU time; with resisting high lossy compression for JPEG at different quality factors (QF), other attacks e.g. Gaussian noise, salt & pepper, rotation attacks and finding the solution using the knowledge of game theory, thus, designing the game matrix to protect the intellectual property rights of owner against the illegal infringement.

This paper is organized in the following manner. Section 2 introduces watermarking as a Game and describes the proposed model elements. Section 3 includes experimental results along with the images, tabular descriptions and graphical analysis. Section 4 and 5 provides conclusion and future work respectively. Section 6 deals with references.

2. Game Theoretic Watermarking System

Watermarking [2,7] models a copyright protection mechanism where an original data sequence is modified before distribution to the public in order to embed some extra information. The embedding should be transparent and robust.

We make the conservative assumption that there is a malicious attacker who knows how the watermarking system works and who attempts to design a forgery that is similar to the original data but that does not contain the watermark.

Thus, *In the n-player normal form game* $G= [N,S,\{U_i\}]$ where,
N - *Set of Players i.e. {encoder, attacker}*
S_i - *Set of Actions Available to Player i*
$S_{encoder}=\{S_1 \text{ to } S_{12}\}$
$S_{attacker}= \{A_1 \text{ to } A_{12}\}$
s_i - *A particular action chosen by i,* $s_i \in S_i$
S - *Action Space*
$\{U_i\}$ – *Set of individual Objective Functions*

$$U_{encoder}= [\alpha \text{ (INFORMATION CONTENT)} + \beta \text{ (COMPLEXITY)}] / \gamma \text{ (DISTORTION)}$$

Where $U_{encoder}$= payoff fuction for encoder,
$\alpha= 0.7\text{-}0.9, \beta= 0.5\text{-}0.6, \gamma= 0.3\text{-}0.4$

$$U_{attacker}= [1-(\text{normalized correlation coefficients of the extracted watermark})]$$

Where $U_{attacker}$= payoff function for attacker

We compute the data for several scenarios, focusing largely on different attacks [7] by the attacker and construct a decision box representing all possible values associated with original image and the decoded one. This decision box will result into the best possible strategy for the encoder to select in order to prevent data from piracy, thus, making the watermarking system more energy efficient. The block diagram of complete system is shown in figure 1 and flow chart of the system is shown in at the end (flow chart 1).

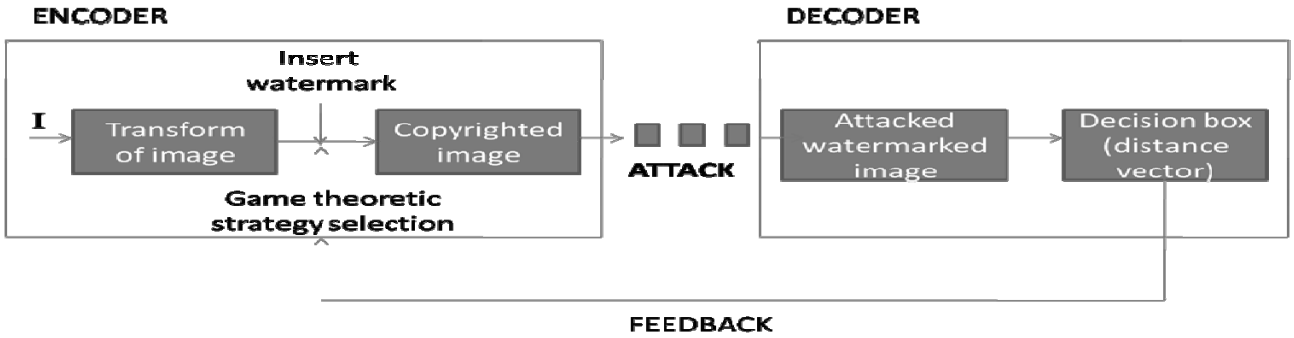


Figure 1. Proposed Watermarking system [1]

2.1. Insertion of watermark

Watermark (W) can be embedded to HL, LH, HH sub-bands at selected levels of decomposition and to LL detail at the third level (Figure 2).

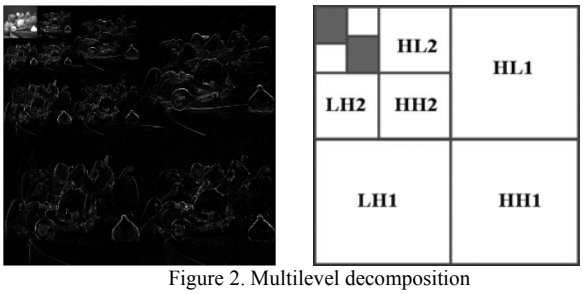


Figure 2. Multilevel decomposition

The embedding rules are:

$W_i' = W_i + \alpha W_i x_i$ *for all pixels in LH, HL*

$W_i' = W_i$ *for all pixels in HH, LL*

Inverse wavelet transform is performed to get the watermarked image, which is transmitted to decoder/receiver.

2.2. Transmission of watermarked image

When the watermarked image is passed through the channel it is vulnerable to various attacks.
Where the channel capacity (X: signal, Y: received signal):

$$C = \max_q I(X;Y)$$

In case of Gaussian channel is given as:

$$C = \frac{1}{2}\log_2\left[1+\frac{P}{N}\right]$$

where N is the noise and P, constrained power is given as:

$$\frac{1}{n}\sum_{i=1}^{n} X_i^2 = P$$

2.3. Extraction of watermark and sensing the attack incurred

To obtain the watermark, the attacked image is again subjected to DWT.

Wq = 1 if { DWT(attacked) – DWT(original) < 0 }
Wq = 0 if { DWT(attacked) – DWT(original) > 0 }

On extracting the watermark and reviewing the initial game matrix residing at the decoder's site, it will be able to sense the optimized strategies based upon a particular distortion threshold value, corresponding to the strategy taken by encoder.
Since the communication channel is dynamic in nature it will update the game matrix and will shift the equilibria each time the attacker introduces some distortion in the image, to have a stable system.
Based upon the following factors, the system will have dynamic configuration: information content, level of complexity of selective strategies and CPU time utilized.

2.4. Feedback Loop

Based upon the computationally optimized results from the decision box, it senses the attack that had been occurred and sends it back to the Game theoretic strategy box at the encoder side. The decision box will choose the optimized feedback, by analyzing the distortion and the correlation between corresponding signal to noise ratios (SNR) using min-max theorem.

$$PSNR = \frac{XY \max_{x,y} p_{x,y}^2}{\sum_{x,y}\left(P_{x,y} - \overline{P}_{x,y}\right)^2}$$

The best attack is the one leading to the worst-case performance [7], i.e.

$$A^* = arg \min_{A \in A} \text{perf}(E, A)$$

And the best defense strategy is:

$$E^* = arg \max_{E \in E} \text{perf}(E, A^*) = arg \max_{E \in E} \min_{A \in A} \text{perf}(E, A)$$

Depending upon the attack, the encoder will incorporate the changes that are require to send the data without prone to any type of attacks, forgery or piracy.

3. Experimental Results

To map watermarking system into game theoretic model for various attacks multiresolution wavelet decomposition is used with four kinds of daubechies (db1-4) at levels 2, 3 and 4. The data is analyzed for three different images based upon their information content.

The host image was first decomposed in the wavelet domain generating four image sub-bands: LL, HL, LH, and HH. Further decomposition of LL level is done to have multilevel decomposition. The watermark is an image of size smaller than the host image. Watermark image is embedded in the host image at the appropriate level and inverse wavelet transform is performed to get the watermarked image.
Figure 3 shows the original and watermarked images used.

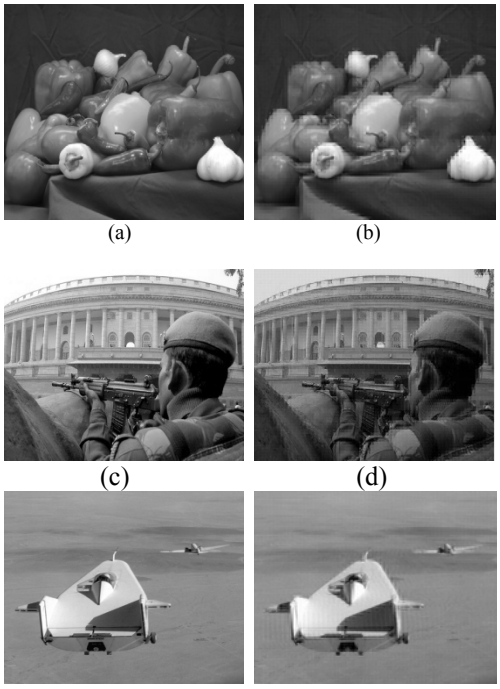


Figure 3. (a) peppers.png, (b) watermarked image of (a), (c) parliament.jpg, (d) watermarked image of (c), (e) liftingbody.png, (f) watermarked image of (e)

Figure 4 shows the embedded watermark.

Figure 4. Watermark

The watermarked image is subjected to various attacks in course of transmission in the channel. The watermark is extracted at the decoder side from the received image and the content of information present is calculated in terms of correlation index with respect to the original watermark. We have analyzed 600 extracted watermark images and their correlation index received for different wavelets and levels. Figure 5 shows the extracted watermark of QF 50%.

Figure 5. Extracted watermark

We have analyzed twenty five tables comprising of correlation coefficients and CPU time out of which db2-level3 values is shown in following table 1.

Attack(↓) / Levels(→)	cv2	ch3	cv3	CPU TIME
JPEG QF 100%	0.9803	0.9044	0.8891	0.2500
JPEG QF 80%	0.9406	0.8512	0.8686	0.1875
JPEG QF 50%	0.4628	0.6341	0.7184	0.2031
JPEG QF 30%	0.2488	0.3428	0.3549	0.2344
JPEG QF 10%	0.0818	0.0410	0.0313	0.2344
BLURRED	0.0174	0.5628	0.0197	0.2500
DEBLURRED	0.7769	0.9116	0.5889	0.2031
ROTATION	0.0079	0.0269	0.0017	0.2344
AVG FILTERED	0.3002	0.6080	0.5912	0.2344
SALT N PEPPER	0.5635	0.3610	0.3742	0.2188
AWGN NOISE	0.2094	0.1758	0.1946	0.2500
MEDIAN	NaN	0.0276	0.0418	0.2188

Table 1. DB2-Level 3 values

Depending upon the data collected an initial game matrix is drawn at the decoder's site comprising of twelve attacks against twelve strategies (taken for experimental ease). Each cell has corresponding payoff values (calculated using the formula in section 2).

This initial game matrix is now updated to maintain the system dynamism, based upon which following cases can be given as:

I. *α-γ or β emphasis:* the payoff value of the encoder is modified using:
   - *α-γ: when information content is important.*
   - *β: when complexity of the system is considered*

II. *Simultaneous changes in above three variables:* the optimal solution for the watermarking game is obtained by simultaneous modifications in α, β, and γ, when all of these are taken into consideration. Thereby obtaining an optimal strategy for the game matrix.

3.1 Game Matrix Analysis

Consider the initial game matrix shown in table 2 representing six strategies v/s six possible attacks. For the selected strategies of the encoder the threshold values (maximum permissible distortion level) corresponding to different attacks is pre determined.

For example- the received watermark has distortion value in the range of 0.6-0.7 and the desired reduction in distortion is 10-15% lesser than the obtained value. Thus, solving the matrix using Iterated Elimination of Strictly Dominated Strategies, expressed as: *In the normal form game* $G=\{S_1 \ldots\ldots S_n: u_1 \ldots\ldots u_n\}$, *let* s_i' *and* s_i'' *be feasible strategies for player i. Strategy* s_i'' *is strictly dominated by* s_i'' *if for each possible combinations of other player's strategies, i's payoff from playing* s_i'' *is strictly less than i's payoff from playing* s_i''*:*

$$U_i(s_1,\ldots,s_{i-1}, s_i', s_{i+1},\ldots s_n) < U_i(s_1,\ldots,s_{i-1}, s_i'', s_{i+1},\ldots s_n)$$

Strat/ Attack	A1	A2	A3	A4	A5	A6
S1	72.73, 0.27	30.40, 0.62	20.00, 0.91	28.90, 0.65	50.59, 0.004	41.78, 0.46
S2	37.27, 0.05	35.98, 0.49	18.13, 0.92	***43.49, 0.41***	48.76, 0.007	54.59, 0.33
S3	46.87, 0.02	32.26, 0.5	20.15, 0.77	33.67, 0.48	47.80, 0.005	53.43, 0.31
S4	30.54, 0.48	19.61, 0.72	14.68, 0.93	18.21, 0.77	46.50, 0.02	20.91, 0.68
S5	48.63, 0.28	19.99, 0.64	13.24, 0.92	30.15, 0.44	45.67, 0.09	34.28, 0.39
S6	46.78, 0.26	21.78, 0.53	12.56, 0.86	22.74, 0.51	28.10, 0.45	29.62, 0.40

Table 2. Game Matrix

We get (S2, A4) as the optimized solution.
Again if a new attack is incurred into the system with the distortion value of 0.8, then the system will update and adapt itself, by computing the new payoffs as per the formula in section2. The updated matrix therefore can be shown as table 3.

Strat/ Attack	A1	A2	A3	A4	A5	A6
S1	24.55, 0.27	23.56, 0.62	22.75, 0.91	23.48, 0.65	14.25, 0.004	***24.02, 0.46***
S2	23.33, 0.05	22.04, 0.49	20.85, 0.92	22.29, 0.41	12.43, 0.007	22.52, 0.33
S3	22.17, 0.02	20.16, 0.5	19.39, 0.77	20.20, 0.48	11.29, 0.005	20.70, 0.31
S4	18.32, 0.48	17.65, 0.72	17.07, 0.93	17.53, 0.77	19.16, 0.02	17.77, 0.68
S5	17.02, 0.28	15.99, 0.64	15.22, 0.92	16.58, 0.44	14.24, .09	16.71, 0.39
S6	15.20, 0.26	14.43, 0.53	13.50, .86	14.49, .51	15.81, .45	14.81, .40

Table 3. Updated Game Matrix

By solving the above matrix iteratively, we get (S1, A6) as the optimized solution, thereby shifting the equilibria across the matrix to the desired state. This is accomplished by varying the parameters (*α, β, or γ*), depending upon the system requirements and thus increasing the payoffs of the optimized strategies, which will be selected to protect the

system from copyright violations, hence establishing the essence of watermarking.

Similarly complete data for 200 images are analyzed to generate the optimal feedback from the decision box to the strategic box using the game matrix. Matrices can be solved using the game theoretic methods like iterative dominance.

5. Conclusion

In this research, we have shown for the first time that how the micro economic game theory can be applied and implemented, in the engineering field, for the resolution of the conflicting behaviors of the devices. We have mapped the water marking system into a "game theoretic watermarking game model", where two rational players i.e. encoder and the attacker rationally choose their strategies in order to maximize and minimize their payoffs, respectively.

This can be used for copyright protection of digital information, undergone various noise attacks, over Internet keeping the band width, memory, processor speed, time, information content and cost limitations in consideration. Using several mathematical models and equations, we have shown how to capture the concerned conflicting watermark security problem into a game theoretic model and we have analyzed the data obtained from the several attacks which are intended to distort the original information, to predict the behavior of the players.

6. Future Work

The proposed research can be extended to color images as well as to audio and video signals. Coding strategies to reduce extracted watermark bit error can also be adopted.

Due to the lack of invariant properties of DWT, it is prone to several geometric attacks like rotation and filtering attacks e.g. median filtering. To improve the reliability of the DWT based watermark detection, we can introduce the new multiresolution-based image registration method that is used to recover the geometrically distorted image before detecting the watermark.

We have considered the non-cooperative incomplete information game strategies, so the model can be extended to cooperative game theory. Also mixed strategies can be incorporated, to check the robustness of the system when one or more attacks are incurred.

7. References

[1]. Akash Tayal, Ashwani Kumar, Ankita Lathey and Shweta, "Watermarking with Multilevel Wavelet Decomposition: Rationality Leads to Conflict Resolution", Security in identity management SIM-09, Indian Institute of Management Ahemadabad, sponsored by Research council of UK (RCUK), pp-111-115.

[2]. Akash Tayal, Ashwani Kumar, Ankita Lathey and Shweta, "Game Theory: Modeling and Analyzing Conflicting Security Applications by Embedding Rationality", IndiaCom-2009, pp. 517-520.

[3]. Akash Tayal, "Game Theory: A Review of Mathematical Economics and application in Internet", International Conference on Recent Advancement of Computer in Electrical Engineering, Bikaner, Rajasthan.

[4]. Ankita Lathey, Akash Tayal and Shweta, "MOBILE COMPUTING: A Smart Application Using J2ME Technology", IndiaCom 2008, pp 320-325.

[5]. MacKenzie, A.B., Wicker S.B., "Game theory in communications: motivation, explanation, and application to power control," IEEE GlobeCom 2001, Nov. 2001, pp. 821-826.

[6]. C. H. Papadimitriou, "Algorithms, Games, and the Internet," Proceedings STOC, 2001

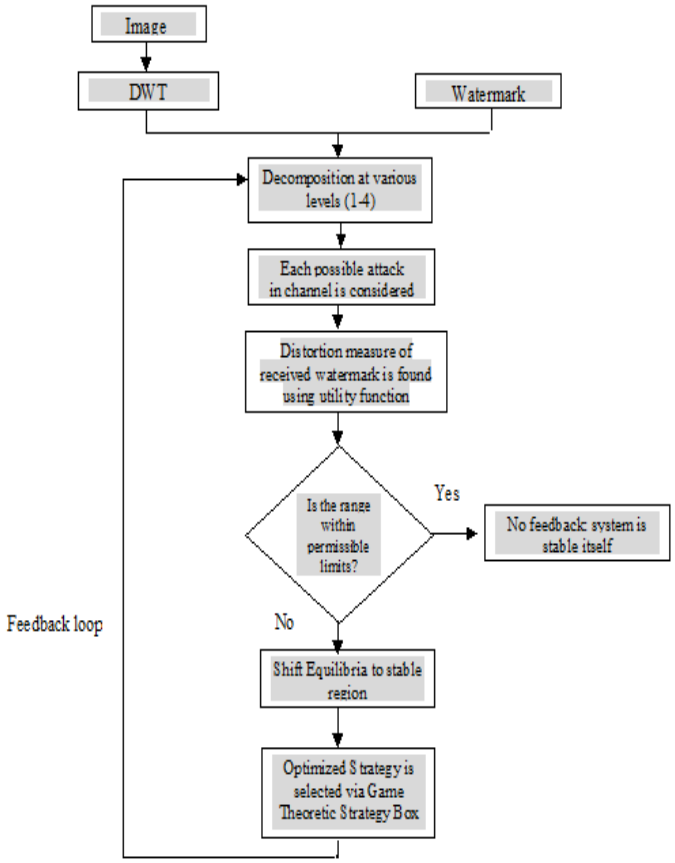
[7]. A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," IEEE Trans. Inform. Theory, vol. 48, no. 6, pp. 1639–1667, Jun. 2002.

[8]. Pierre Moulin and Ralf Koetter, "Data-Hiding Codes", IEEE proceedings, vol. 93, no. 12, December 2005.

[9]. R. Gibbons, "A Primer in Game Theory". Prentice Hall, 1992.

[10].M. J. Osborne and A. Rubinstein, "A Course in Game Theory". Cambridge, MA: The MIT Press, 1994.

[11].Watermarking Systems Engineering**,** By Mauro Barni.



Flow chart 1. System Overview

SHWETA received the B.Tech degree in Computer Science and Engineering from Indira Gandhi Institute of Technology, Guru Gobind Singh Indrapastha University, Delhi, India in 2009. She is presently working with Department of Information Technology, Delhi Technological University (Formerly Delhi College of Engineering), Delhi, India as Assistant Professor. Her research interest includes Digital Image Processing, Watermarking, Soft Computing and Cloud Computing.

AKASH TAYAL received the B.Tech degree from Jamia Millia Islamia, Delhi, India and M.Tech degree from Netaji Subhash Institue of Technology, Delhi University, Delhi, India in 2002. He has over 7 years teaching experience. He is presently working with Department of Electronics and Communication Engineering, Indira Gandhi Institute of Technology, Guru Gobind Singh Indrapastha University, Delhi, India as Assistant Professor. He has published around 20 research papers in reputed Conferences and Journals. His research interest includes Digital Image Processing, Optimization and non-linear statistical processing.

ANKITA LATHEY received the B.Tech degree in Computer Science and Engineering from Indira Gandhi Institute of Technology, Guru Gobind Singh Indrapastha University, Delhi, India in 2009. She is presently working with FIITJEE Limited, India as Senior Lecturer and Content Developer/ Research Analyst for USA UnivQuest program. Her research interest includes Digital Image Processing, Watermarking and Mobile Computing.