Expert Systems with Applications 38 (2011) 5748–5754

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

A game-theoretic framework for the security system of visible watermarking

Min-Jen Tsai*, Jung Liu, Chen-Sheng Wang

Institute of Information Management, National Chiao Tung University, 1001 Ta-Hsueh Road, Hsin-Chu 300, Taiwan, R.O.C.

ARTICLE INFO

Keywords:
Copyright protection
Game theory
Nash equilibrium
Digital watermarking
Wavelet

ABSTRACT

Perfect digital watermarking systems are contained two characteristics. One is the robustness that it need be resistant to geometric attacks in addition to common image processing tasks, such as JPEG compression. The other one is to preserve the image quality after embedding. However, the requirement of robustness and quality for watermark are conflicted with each other. How to determine the equilibrium of optimal security strategies between encoder and attacker and the optimal tradeoff between the intensity of embedded watermark and the perceptual translucence for visible watermark is still remained as one of the most challenging research topics in image watermarking. Therefore, in order to achieve the best tradeoff between the embedding energy of watermark, the quality of perceptual watermark translucence and the image fidelity after attacks, we propose a system architecture which is based on the game-theoretic approach that provides an optimum solution for the decision maker by studying the intensity and perceptual efficiency. The game-theoretic approach determines the transmission strategy using utility optimization according to the fluctuation of watermark states. The watermark embedding problem is formulated as a dynamic non-cooperative game with complete information while the optimal strategy is defined by the Nash equilibrium of the game. The experimental results demonstrate the feasibility of the proposed approach which allows the watermark encoder to obtain the best adaptive watermarking strategy in the different texture under attacks. Additionally, we demonstrate that the proposed system could help each user to choose the optimal transmission power to maximize its utility based on other constant parameters and resolve security issue of visual communication.

1. Introduction

The knowledge-based economy has become the major trend in international society in the 21st century. Exploring the characteristics of the knowledge-based economy and establishing an appropriate economic paradigm for accelerating technological innovation is an urgent task for copyright ownership. Therefore, intellectual property becomes the critical issue of property owner concern. Books, music, digital multimedia, and any kind of arts actually belong to the authors who made it, and the authors have the rights to restrict access to intellectual property (WIPO).

With the advantages of easy editing and reproduction of digitalized data, the protection of the intellectual rights and the authentication of digital multimedia no doubt have become issues of great importance in recent years (Cox, Miller, Bloom, Fridrich, & Kalker, 2007; Kundur, Lin, Macq, & Yu, 2004). Digital watermarking has been extensively studied and regarded as a potentially effective means for protecting copyright of digital multimedia in recent years. Visible watermarking schemes protect copyrights in a more active way. For example, they not only prevent pirates but also recognize the owner of the multimedia. However, robustness and quality for a digital content and watermark are conflicted with each other. Consequently, applications of visible watermarking are often limited to content browsing or previewing.

The study we present in this paper is an attempt to explore the problems of these earlier studies on visible watermarking and propose a novel security architecture based on game-theoretic methodology that provide an optimum solution for the copyright manager to make a decision by studying in effect of transmission power on intensity and perceptual efficiency. We have formulated the watermark embedding problem as a dynamic non-cooperative game with complete information (Osborne, 2003). Complete information requires that every player know the strategies of the other players but not necessarily the actions. Under the complete information, we present a watermarking game to analyze the different situation and get the optimal strategy between the embedding energy of watermark and the perceptual translucence for visible watermark.

The rest of this paper is organized as follows. In Section 2, related works and the detailed description of the proposed watermarking system architecture will be explained. In Section 3, numerical results with discussion illustrate the basic ideas of the proposed approach. Finally, the conclusion is drawn in Section 4.

* Corresponding author. Tel.: +886 3 571 2121x57406; fax: +886 3 572 3792.
E-mail address: mjtsai@cc.nctu.edu.tw (M.-J. Tsai).

0957-4174/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2010.10.058

2. The game-theoretic framework

2.1. Game theory

Game theory is the formal study of the conflict and cooperation. The concepts of game-theoretic approach help to formulate structure, analyze and understand strategic scenarios and make a decision whenever the actions of the several agents are interdependent (Osborne, 2003). Game theory aims to help us understand situations in which decision-makers interact. Therefore, decision-makers can better estimate the potential effects of their actions and then make the optimal decisions to avoid the conflict.

In game theory, Nash equilibrium is a solution concept of a game involving two or more players, in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only his or her own strategy unilaterally. If each player has chosen a strategy and no player can benefit by changing his or her strategy while the other players keep theirs unchanged, then the current set of strategy choices and the corresponding payoffs constitute Nash equilibrium (Osborne, 2003). We will describe how we can apply such concept to make the game design for making decision of the visible watermark embedding procedures.

2.2. Visible watermarking approach

Regarding the digital watermarking techniques, Fig. 1 describes the generic structure for visible watermark embedding processes. First, a host image (original image) directly embeds watermark in spatial domain or is transformed into frequency domain through the well-known spread spectrum approach (Cox, Kilian, Leighton, & Shamoon, 1997), i.e. DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) (Mohanty, Ramakrishnan, & Kankanhalli, 2000) or DWT (Discrete Wavelet Transform) (Cox et al., 2007; Huang & Tang, 2006; Kundur et al., 2004; Tsai, 2009). However, the algorithms using transform domain approach develop more robust watermarking techniques than directly embedding watermark into the spatial domain (Chen, 2000; Cox et al., 2007). Consequently, coefficients are passed through a perceptual analysis block that determines how strong the watermark in embedding algorithm can be, so that the resulting watermarked image is acceptable. The watermark is embedded through using a well-designed algorithm based on mathematical or statistical model. If the host image is employed in frequency domain, the inverse spread spectrum approach is then adopted to obtain a watermarked image (Huang & Tang, 2006; Tsai, 2009). The watermark extraction applies to the similar operations in embedding processes with reverse procedures.

Regardless of exploiting the visible watermarking technique, the watermarked image can generally be formulated as shown in Eq. (1)

$$I^{w}_{x,y} = \alpha_{x,y} \times I_{x,y} + \beta_{x,y} \times w_{x,y} \tag{1}$$

where $I_{x,y}$, $I^{w}_{x,y}$ and $w_{x,y}$ are the (x, y)th pixels of the host image, the watermarked image, and the visible watermark logo image, respectively, and $\alpha_{x,y}$ and $\beta_{x,y}$ are the two weighting factors. In most of the visible watermarking methods, all weighting factors are usually variables. While the image quality of $I^{w}_{x,y}$ is a constraint during the watermark embedding, the selection of $\alpha_{x,y}$ and $\beta_{x,y}$ will be critical since they both will be comprised for the expected image quality of $I^{w}_{x,y}$. After the watermark embedding stage, the attackers would try different attack to remove the watermark and the robustness of the watermarking technique is essential to protect the intellectual property. Therefore, the visible watermark embedding problem can be stated as a non-cooperative game where individual player decide the strategy to cope with the difference situation. In this study, an up-to-date visible watermarking technique named "COCOA" (Tsai, 2009) is adopted in this research which is based on the content and contrast aware (COCOA) technique with the consideration of Human Visual System (HVS) model. Interested reader can refer (Tsai, 2009) for more technical information.

In order to get the optimal strategies in various situations, an example is shown in Fig. 2 where the amount of intensity increases, the watermark quality also increases as well as the robustness against attacks. Consequently, the successful ratio of attacker is decreasing and an equilibrium condition exists when the optimal strategies are encountered for both sides.

To utilize the game theory architecture into the watermark security architecture, each player's profit is determined by the payoff function and Fig. 3 demonstrates the complete diagram of the game-theoretic security system architecture for two players – encoder and attacker. Their roles and function are described as follows:

A game-theoretic security system consists of

- a set of players,
- for each player, each has a set of actions,
- for each player, there are a set of constraints,
- for each player, there is existing a payoff function to estimate each profit.

2.2.1. Players

In this case, there are two players. One player is the encoder player and the other one is the attacker player.

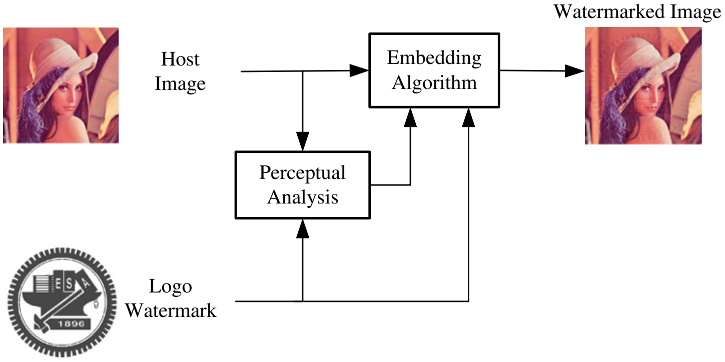

Fig. 1. A generic visible watermark embedding diagram.

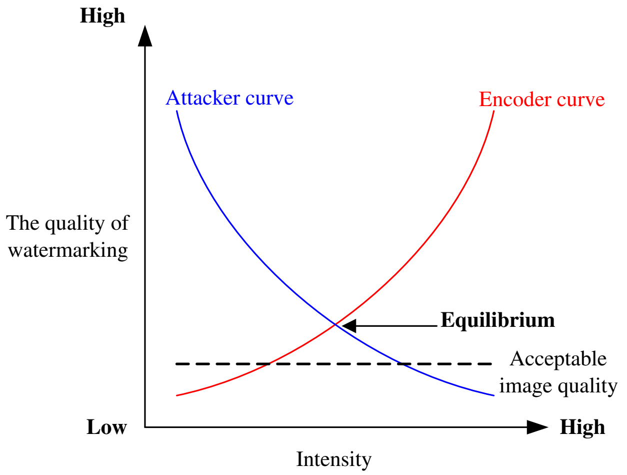

Fig. 2. The equilibrium illustration of optimal security strategies between encoder and attacker.

2.2.2. The constraints

There exists the constraint for the receiver where the image quality of attacked watermarked image is concerned. If the image quality is not satisfactory, the receiver won't accept it and will request the encoder to resend the image. On the other hand, the attacker player cares the destruction of the watermark with the acceptable image quality.

2.2.3. Strategies/Actions

Due to the dynamic property for determining the best parameters during the watermark embedding stage, there are certain strategies/actions for each player.

Let *i* and *j* denote the state of encoder and attacker players. The set of strategies for encoder player is {*i*, *i* = 1, 2, 3, ... , 11} which contains 11 different parameter selections for COCOA visible watermarking. On the other hand, we assume that attacker adopts the technique to remove or destroy the watermark from the watermarked image. In this research, we only consider JPEG2000 compression but the approach can be extended to other attacks. Here the set of actions for attacker player is {*j*, *j* = 1, 2, 3, ... , 11} where they are equivalent to compression ratio of no compression, 0.1, 0.09, . . . , 0.01 for total 11 states. The meaning of compression ratio like 0.01 represents 100:1 between the uncompressed image and compressed image. Other setting of 0.1–0.02 has the same operation.

2.2.4. Payoffs

The payoff represents the welfare of the players at the end of the game. They are the basis on which each player chooses his strategy. In this approach, the payoff of a player is defined as the total profit which is the sum of the individual player's profits from actions. From encoder player point of view, the peak signal noise ratio (*PSNR*) between the host image and the watermarked image is critical since the encoder expects the highest fidelity after watermark embedding. In addition, the correlation between the logo watermark and the extracted watermark after attack is also important since the robustness of the watermark embedding technique is also concerned for encoder player. Therefore, *PSNR* and *correlation* functions will be adopted in the payoff function for encoder player.

The payoff function f_1 of encoder player is defined as a function of the strategy profiles e_1 (*PSNR*) and e_2 (*correlation*) as shown in Eq. (2)

$$f_1(i,j) = \frac{e^1_{i,j} - min\left(e^1_{.,j}\right)}{Max\left(e^1_{.,j}\right) - min\left(e^1_{.,j}\right)} + \frac{e^2_{i,j} - min\left(e^2_{.,j}\right)}{Max\left(e^2_{.,j}\right) - min(e^2_{.,j})} \qquad (2)$$

where $e^1_{i,j} = PSNR(I, I_w)_{i,j}$, $e^2_{i,j} = correlation((I_w - I), w)_{i,j}$.

The meaning of $e^1_{.,j}$ represents the payoff value of certain *j* for whole set {*i*, *i* = 1, 2, 3, ... , 11}.

Note:

I is the original host image.
w is the logo watermark.
I_w is watermarked image.
I'_w is the attacked watermarked image.

The payoff function f_1 is actually a normalized operation from *PSNR* and *correlation* in order to get a balanced function value. The encoder's best response function is $f_1^* = \max f_{1(.,j)}$.

From attacker player point of view, the peak signal noise ratio (*PSNR*) between the watermarked image and the attacked watermarked image is critical since the attacker expects the lowest image quality after watermark attack. Hence, the payoff function of attacker player, f_2 can be defined as Eq. (3)

$$f_2(i,j) = PSNR\left(I_w, I'_w\right)_{i,j} \qquad (3)$$

The attacker's best response function is $f_2^* = \min f_{2(i,.)}$.

2.2.5. Optimal solution

Nash equilibrium is widely considered as the solution of the non-cooperative static games and we apply the extended solution

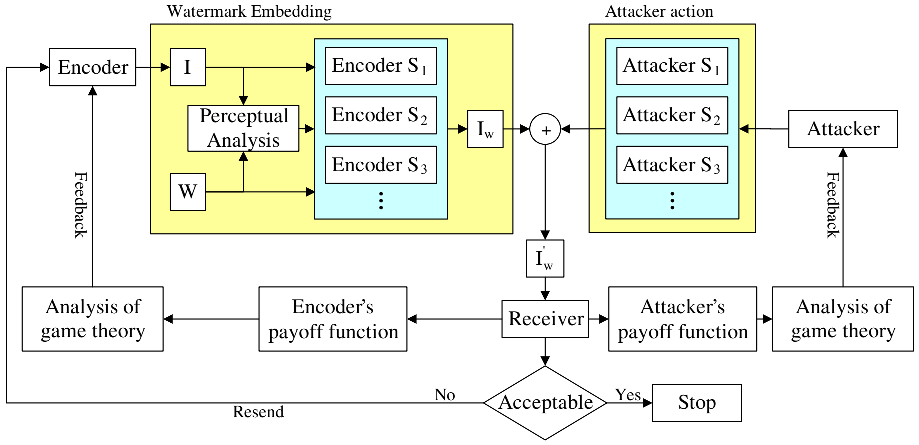

Fig. 3. The complete diagram of the game-theoretic security system design for two players – encoder and attacker.

concept of the game perfect equilibrium to analyze the strategic behaviors of the players in the watermark embedding stage that is characterized as a dynamic game. If there is a solution profile (f_1^*,f_2^*), we can say (f_1^*,f_2^*) is an optimal solution of the game.

3. Experimental results and discussions

In this section, experimental results are given to illustrate the powerful game-theoretic system that provides decision maker to get an optimum solution on the perceptual watermark transparency and robustness against JPEG compression. The proposed game-theoretic system security design has been implemented and widely examined. The COCOA visible watermarking algorithm (Tsai, 2009) has been adopted in this research and intensively tested by using the commonly available colour images from the USC image database (USC SIPI). A more detailed understanding of the embedded grayscale logo watermark is illustration in Fig. 1 which is the school logo. Fig. 4 shows some sample images (Lena and Lake images) from USC SIPI and the watermarked image using COCOA algorithm.

For demonstration the purposed a security system based on game-theoretic approach in the visible watermarking, we use COCOA visible watermarking algorithm and a wide range of security attack pattern by different JPEG compression. As we have seen, it is reasonable to assume that the encoder is know the potential attack actions and encoder hope to gain a better strategy between the embedding energy of watermark, the quality of perceptual watermark translucence and the image fidelity after attacks.

The proposed game-theoretic system security design has been implemented and widely examined. The COCOA visible watermarking algorithm (Tsai, 2009) has been adopted in this research and intensively tested by using the commonly available colour images from the USC image database (USC SIPI). The embedded grayscale logo watermark is illustration in Fig. 1 which is the school logo. Fig. 4 shows a sample image from USC SIPI and the watermarked image using COCOA algorithm.

For demonstration purpose, Tables 1 and 2 tabulates e_1 (*PSNR*) and e_2 (*correlation*) payoff values from different encoder's strategies and attacker's actions for Lena image (Fig. 4(b)). Table 3 illustrates the encoder's payoffs and the optimal selection for various function values $f_1(i,j)$. From Table 3, the best selection from encoder for each attacker action j occurs between different encoder strategy i which is marked by *. It characterizes the goal of the encoder is not only achieving the highest perceptual image quality but also enduring the watermark robustness against the attacker.

Table 4 demonstrates the optimal solution of the Nash equilibrium state from the encoder's payoffs and the attacker's payoffs under the game-theoretic security decision system. Without the constraint of attacked watermarked image, the optimal solution is at the state of $(i,j) = (5,11)$ for Lena image which is equivalent to 28.444 dB image quality under 100:1 JPEG2000 compression attack with f_1 value of 1.215. If the quality of the attacked watermark image is concerned and we set the acceptable *PSNR* value at 30 dB as a threshold, the best selection will be $(i,j) = (6,9)$ which will achieve 32.68 dB under JPEG2000 compression with the compression ratio of 100:3 attack with f_1 value of 1.339. Similar game-theoretic design for Lake image (Fig. 4(d)) is also performed and tabulated the payoff results in Table 5. Without the constraint of attacked watermarked image, the optimal solution is at the state of $(i,j) = (7,11)$ for Lake image which is equivalent to 24.353 dB image quality under 100:1 JPEG2000 compression attack with f_1 value of 1.209. While the acceptable PSNR value at 30 dB is set, the best selection will be $(i,j) = (6,7)$ which will achieve 30.591 dB under JPEG2000 compression with the compression ratio of 100:5 attack with f_1 value of 1.299.

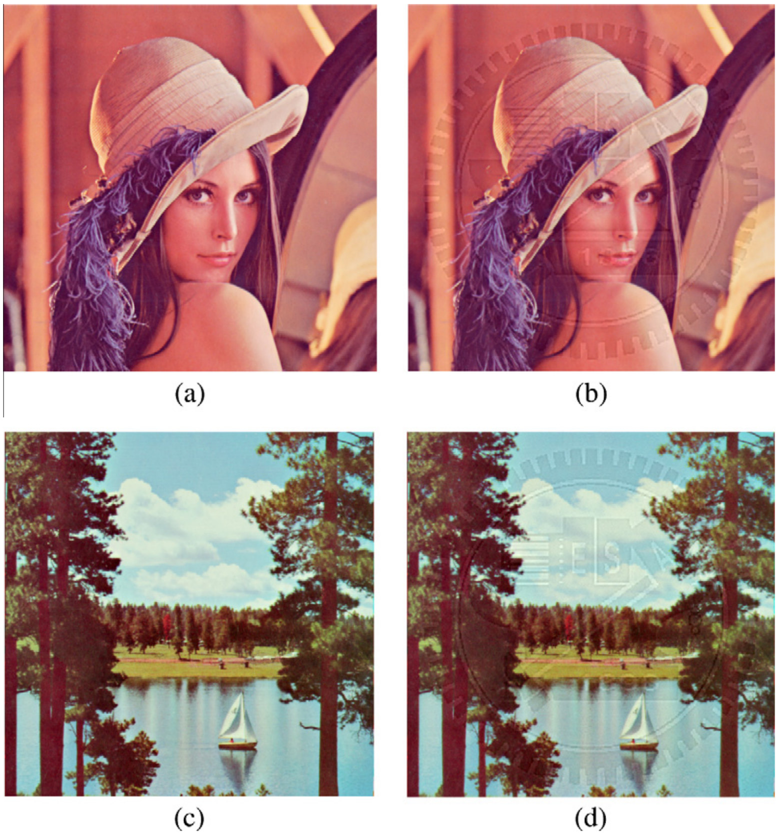

Fig. 4. (a) Original Lena image. (b) Watermarked Lena image. (c) Original Lake image. (d) Watermarked Lake image.

Table 1
PSNR(dB) summary in different encoder's strategies and attacker's actions.

	i	Attacker *j*										
		1	2	3	4	5	6	7	8	9	10	11
Encoder	1	57.94	38.38	37.94	37.40	36.83	36.09	35.33	34.25	33.04	31.08	28.29
	2	47.00	37.89	37.49	37.03	36.47	35.75	35.02	34.10	32.90	30.88	28.31
	3	42.04	36.85	36.65	36.30	35.87	35.33	34.57	33.70	32.58	30.79	28.10
	4	38.77	35.51	35.40	35.23	34.94	34.58	33.92	33.24	32.25	30.54	28.07
	5	36.39	34.16	34.07	33.92	33.74	33.46	33.11	32.55	31.70	30.31	27.89
	6	34.52	32.86	32.72	32.60	32.42	32.19	32.05	31.88	31.20	29.87	27.65
	7	32.99	31.75	31.62	31.51	31.32	31.11	31.09	30.95	30.56	29.49	27.41
	8	31.69	30.67	30.58	30.42	30.24	30.19	30.15	30.02	29.92	28.97	27.11
	9	30.55	29.67	29.57	29.48	29.44	29.32	29.31	29.19	29.21	28.60	26.75
	10	29.56	28.78	28.71	28.71	28.69	28.57	28.48	28.47	28.33	28.11	26.36
	11	28.66	27.99	27.94	27.97	27.84	27.78	27.74	27.78	27.73	27.61	26.20

Table 2
Correlation summary in different encoder's strategies and attacker's actions.

	i	Attacker *j*										
		1	2	3	4	5	6	7	8	9	10	11
Encoder	1	0.122	0.004	0.005	0.008	0.003	0.005	0.002	0.001	0.000	0.000	0.002
	2	0.656	0.195	0.179	0.169	0.160	0.152	0.138	0.112	0.093	0.076	0.053
	3	0.685	0.349	0.325	0.301	0.283	0.258	0.240	0.207	0.172	0.132	0.088
	4	0.705	0.455	0.430	0.409	0.382	0.352	0.332	0.283	0.243	0.186	0.129
	5	0.713	0.528	0.513	0.499	0.478	0.448	0.412	0.365	0.322	0.255	0.167
	6	0.717	0.580	0.568	0.551	0.528	0.502	0.475	0.431	0.383	0.301	0.208
	7	0.721	0.619	0.602	0.587	0.567	0.543	0.525	0.486	0.442	0.363	0.248
	8	0.723	0.640	0.628	0.612	0.590	0.574	0.553	0.520	0.487	0.409	0.292
	9	0.725	0.656	0.644	0.634	0.620	0.608	0.585	0.553	0.529	0.453	0.333
	10	0.726	0.668	0.660	0.655	0.645	0.626	0.598	0.576	0.541	0.496	0.363
	11	0.728	0.673	0.668	0.665	0.655	0.635	0.614	0.598	0.558	0.520	0.399

Table 3
The encoder's payoffs and the optimal selection.

	i	Attacker *j*										
		1	2	3	4	5	6	7	8	9	10	11
Encoder	1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99
	2	1.51*	1.24	1.22	1.21	1.20	1.19	1.18	1.16	1.14	1.09	1.13
	3	1.39	1.37	1.35	1.33	1.32	1.31	1.29	1.26	1.22	1.17	1.12
	4	1.31	1.40*	1.39*	1.38*	1.37	1.37	1.35	1.32	1.28	1.20	1.21
	5	1.24	1.38	1.38	1.38	1.39*	1.39*	1.38*	1.35	1.32	1.27*	1.22*
	6	1.18	1.33	1.33	1.32	1.32	1.32	1.34	1.35*	1.34*	1.23	1.21
	7	1.14	1.28	1.27	1.26	1.25	1.26	1.30	1.30	1.32	1.24	1.19
	8	1.10	1.21	1.20	1.18	1.17	1.19	1.22	1.22	1.28	1.18	1.16
	9	1.06	1.14	1.13	1.11	1.13	1.14	1.16	1.14	1.23	1.16	1.09
	10	1.03	1.07	1.07	1.06	1.08	1.08	1.07	1.07	1.08	1.10	0.99
	11	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Without loss of generality, the experimental results show similar behavior which provides the best selection of Nash equilibrium under different attacks. Current experimental results have demonstrated that such game-theoretic system security design for visible watermarking is an effective approach for efficient visual communication in applications. In summary, the proposed technique can resolve the issue for watermark encoder to obtain the best watermarking strategy under attacks.

3.1. Discussions

In this section, we will discuss some possible situations in the game-theoretic architecture system.

(1) Multiple solutions in the game-theoretic architecture system.
Each image has different content or characteristic; the system may have multiple solutions after Nash equilibrium. When the multiple optimal outputs exist, we can assume robustness watermarking is the best response for encoder players. Therefore, encoder will choose the strongest parameter of embedded energy for the decision maker.

(2) No optimal output in the game-theoretic security system.
Similar to multiple solutions, different images might have varied results. The original image involves wide range of characteristics, like complex/simple content or texture and if the quality of watermarked image is around 30 dB, it is

Table 4
Payoff function value with PSNR metric for Lena image under JPEG2000 attack and the optimal selection of *(i, j)* is (6, 9) for acceptable image quality threshold 30 dB, (5, 11) with no image quality constraint.

	i	Attacker *j*										
		1	2	3	4	5	6	7	8	9	10	11
Encoder	1	1.000, 57.936	1.000, 38.367	1.000, 37.926	1.000, 37.385	1.000, 36.812	1.000, 36.071	1.000, 35.316	1.000, 34.238	1.000, 33.034	1.000, 31.076	0.990, 28.290
	2	1.508, 46.995	1.238, 38.377	1.217, 37.890	1.206, 37.370	1.200, 36.795	1.193, 36.084	1.180, 35.325	1.162, 34.343	1.139, 33.116	1.087, 31.075	1.130, 28.447
	3	1.385, 42.035	1.367, 38.293	1.354, 37.819	1.330, 37.259	1.323, 36.746	1.311, 36.097	1.287, 35.305	1.261, 34.335	1.220, 33.098	1.169, 31.196	1.118, 28.388
	4	1.306, 38.772	1.396, 38.131	1.388, 37.600	1.380, 37.106	1.371, 36.513	1.370, 35.874	1.352, 35.128	1.316, 34.187	1.284, 33.048	1.202, 31.185	1.205, 28.492
	5	1.240, 36.385	1.377, 38.023	1.380, 37.495	1.378, 36.894	1.385, 36.327	1.388, 35.616	1.379, 34.891	1.347, 33.944	1.323, 32.834	1.269, 31.179	1.215, 28.444
	6	1.182, 34.523	1.328, 37.945	1.328, 37.306	1.318, 36.716	1.315, 36.050	1.320, 35.338	1.341, 34.597	1.354, 33.644	1.339*, 32.679*	1.229, 30.994	1.206, 28.350
	7	1.136, 32.989	1.280, 37.826	1.269, 37.231	1.257, 36.663	1.252, 35.897	1.255, 35.143	1.297, 34.361	1.302, 33.340	1.323, 32.357	1.240, 30.859	1.194, 28.260
	8	1.095, 31.685	1.208, 37.761	1.204, 37.166	1.181, 36.558	1.168, 35.714	1.193, 34.997	1.218, 34.117	1.215, 33.121	1.283, 32.103	1.179, 30.573	1.163, 28.162
	9	1.059, 30.554	1.136, 37.606	1.127, 36.966	1.113, 36.393	1.125, 35.580	1.142, 34.865	1.160, 33.906	1.142, 32.821	1.225, 31.791	1.156, 30.370	1.094, 27.961
	10	1.028, 29.556	1.068, 37.500	1.067, 36.961	1.064, 36.267	1.078, 35.508	1.081, 34.733	1.072, 33.663	1.070, 32.547	1.082, 31.434	1.098, 30.110	0.987, 27.686
	11	1.000, 28.664	1.000, 37.432	1.000, 36.861	1.000, 36.125	1.000, 35.309	1.000, 34.442	1.000, 33.385	1.000, 32.364	1.000, 31.146	1.000, 29.784	1.000, 27.681

Table 5
Payoff function value with PSNR metric for Lake image under JPEG2000 attack and the optimal selection of *(i, j)* is (6, 7) for acceptable image quality threshold 30 dB, (7, 11) with no image quality constraint.

	i	Attacker *j*										
		1	2	3	4	5	6	7	8	9	10	11
Encoder	1	1.000, 61.586	1.000, 33.107	1.000, 32.730	1.000, 32.149	1.000, 31.453	1.000, 30.808	1.000, 30.139	1.000, 29.135	0.993, 27.923	0.942, 26.350	1.000, 23.886
	2	1.472, 47.361	1.155, 33.308	1.134, 32.909	1.123, 32.305	1.117, 31.635	1.116, 31.010	1.112, 30.328	1.109, 29.331	1.098, 28.142	1.073, 26.610	1.037, 24.012
	3	1.379, 41.888	1.244, 33.460	1.236, 33.081	1.232, 32.503	1.238, 31.827	1.220, 31.169	1.211, 30.484	1.175, 29.438	1.168, 28.269	1.150, 26.717	1.136, 24.101
	4	1.290, 38.503	1.315, 33.539	1.304, 33.142	1.309, 32.612	1.300, 31.931	1.263, 31.217	1.263, 30.571	1.237, 29.568	1.222, 28.376	1.189, 26.794	1.184, 24.197
	5	1.224, 36.066	1.343, 33.628	1.330, 33.191	1.341, 32.641	1.323, 31.891	1.314, 31.287	1.291, 30.577	1.256, 29.614	1.230, 28.423	1.173, 26.827	1.179, 24.244
	6	1.171, 34.163	1.313, 33.630	1.307, 33.184	1.328, 32.608	1.342, 31.912	1.308, 31.245	1.299*, 30.591*	1.247, 29.613	1.223, 28.449	1.200, 26.861	1.207, 24.309
	7	1.126, 32.603	1.270, 33.706	1.267, 33.220	1.298, 32.630	1.305, 31.901	1.287, 31.194	1.297, 30.578	1.262, 29.656	1.253, 28.514	1.264, 26.975	1.209, 24.353
	8	1.088, 31.281	1.205, 33.755	1.209, 33.304	1.236, 32.622	1.240, 31.862	1.249, 31.187	1.251, 30.488	1.225, 29.631	1.216, 28.473	1.215, 26.944	1.174, 24.374
	9	1.055, 30.135	1.144, 33.858	1.141, 33.353	1.158, 32.636	1.168, 31.828	1.163, 31.161	1.182, 30.437	1.179, 29.515	1.173, 28.441	1.142, 26.868	1.142, 24.388
	10	1.026, 29.124	1.080, 33.900	1.079, 33.405	1.079, 32.647	1.086, 31.805	1.087, 31.104	1.103, 30.360	1.098, 29.424	1.104, 28.356	1.099, 26.810	1.088, 24.357
	11	1.000, 28.219	1.000, 33.924	1.000, 33.426	1.000, 32.558	1.000, 31.791	1.000, 31.031	1.000, 30.254	1.000, 29.314	1.000, 28.195	1.000, 26.715	1.000, 24.331

hard to keep the quality of image above the threshold of acceptable image quality after attacker actions. On the other hand, it is possible that no solution exists after the game-theoretic security system. Therefore, attackers can not do anything in the game-theoretic security system.

(3) New attacked actions.
Along with environment vicissitude, the attacker might have new behaviors. In advance, we cannot know every action from attackers to against all attacks. It is the flexibility in the proposed game-theoretic security system, users can extend the actions from attackers or encoders to simulate the actual attacking method and reduce the harm.

4. Conclusions

A need for the best digital watermarking is essential for copyrighted materials which can protect the copyright ownership. In this paper, we have outlined the necessary characteristics of a watermark like robustness to common signal processing operations, and acceptable image quality.

To meet these requirements, we have proposed a visible watermarking system which is based on the game-theoretic architecture that provides an optimum solution for the decision maker by studying in effect of transmission power on intensity and perceptual efficiency. The framework enables us to analyze the actual competition between encoder player and attacker player. In the dynamic non-cooperative situations, it also provides the solution to acquire the optimal selection between transparency and robustness for digital contents in different strategies with complete information.

We expect the proposed approach can provide players of watermarking with useful information on determining their optimal strategy. Based on the results of this paper, one can investigate to obtain more precise representations as well as more efficient solution procedure for the problem in the future. In conclusion, the proposed game-theoretic technique provides a useful decision methodology for encoder who can make the best selection among choices. Accordingly, our research could help each player to choose the optimal transmission power to maximize its utility payoff based on other constant parameters and resolve security issue of visual communication.

Acknowledgments

This work was partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC99-2410-H-009-053-MY2.

Partial technical background is presented in the 2010 ACM Multimedia Conference (Tsai and Liu, 2010).

References

Chen, P. M. (2000). A visible watermarking mechanism using a statistic approach. In *Proceedings of the international conference on signal processing (ICSP)* (vol. 2, pp. 910–913), Aug. 2000.

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing, 6*(12), 1673–1687.

Cox, I. J., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography* (2nd ed.). Morgan Kaufmann.

Huang, B. B., & Tang, S. X. (2006). A contrast-sensitive visible watermarking scheme. *IEEE MultiMedia, 13*(2), 60–66.

Kundur, D., Lin, C. Y., Macq, B., & Yu, H. (2004). Special issue on enabling security technologies for digital rights management. In *Proceedings of the IEEE* (pp. 879–882), June 2004.

Mohanty, S. P., Ramakrishnan, K. R., & Kankanhalli, M. S. (2000). A DCT domain visible watermarking technique for images. *IEEE International Conference on Multimedia and Expo, 2*, 1029–1032.

Osborne, M. J. (2003). *An introduction to game theory*. Oxford University Press.

Tsai, M. J. (2009). A visible watermarking algorithm based on the content and contrast aware (COCOA) technique. *Journal of Visual Communication and Image Representation, 20*(5), 323–338.

Tsai, M. J. & Liu, J. (2010). A game-theoretic system security design for the visible watermarking. In *Multimedia in forensics, security and intelligence – MiFor2010, ACM Multimedia*, Oct 25–29, Firenze, Italy.

USC SIPI – The USC-SIPI Image Database. [Online]: http://sipi.usc.edu/database/database.html.

World Intellectual Property Organization (WIPO), [Online]: http://www.wipo.int/.