International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:9, 2011

The Optimal Equilibrium Capacity of Information Hiding Based on Game Theory

Ziquan Hu, Kun She, Shahzad Ali, and Kai Yan

Abstract—Game theory could be used to analyze the conflicted issues in the field of information hiding. In this paper, 2-phase game can be used to build the embedder-attacker system to analyze the limits of hiding capacity of embedding algorithms: the embedder minimizes the expected damage and the attacker maximizes it. In the system, the embedder first consumes its resource to build embedded units (EU) and insert the secret information into EU. Then the attacker distributes its resource evenly to the attacked EU. The expected equilibrium damage, which is maximum damage in value from the point of view of the attacker and minimum from the embedder against the attacker, is evaluated by the case when the attacker attacks a subset from all the EU. Furthermore, the optimal equilibrium capacity of hiding information is calculated through the optimal number of EU with the embedded secret information. Finally, illustrative examples of the optimal equilibrium capacity are presented.

Keywords—2-Phase Game, Expected Equilibrium damage, Information Hiding, Optimal Equilibrium Capacity.

I. Introduction

IN the information hiding technique, first we embed the secret information into the digital signal such as audio, image and video, and then pass this secret information through the open channel. Robustness, undetectability and capacity are three most important factors of information hiding [1]-[5]. There are numerous important methods proposed by the researchers, concerning these questions. Cooperman M. and Moskowitz S. embedded the information into the Least Significant Bit or Bits [6]. Q. Li and I. J. Cox proposed the method inserting the digital watermarking into the domain of Discrete Cosine Transform [7]. In [8], L. M. Marvel, C. G. Boncelet Jr. and C. T. Retter wrote the secret information in the spread spectrum of the image. W. Bender, D. Gruhl and N. Morimoto embedded the secret information in patchwork [9]. S. Pereira and T. Pun presented a fast robust template matching for affine resistant image watermarks [10]. And T. Aura used mimic function to insert the secret information into the carrier based on the generation technique [11]. In these methods the embedder applied the different algorithms to deploy the secret information into the signal so that the embedder could conceal the secret information in the digital signal and the secret information couldn't be detected by the attacker.

However, how much secret information should be embedded into the signal when the attacker has options of attack strategies? There is a need to go beyond earlier research. This paper assumes that the embedder and the attacker have their own limited resources respectively and they are fully strategic optimized agents, and that the former minimizes the expected damage caused by the attacker, while the latter maximizes the damage. This conflicted issue may be solved by applying the game theory which can analyze the conflicted questions [12]-[14]. In this paper 2-phase game theory includes the embedder, building the embedder-attacker system and other one is the attacker who destructs the system. The embedder first consumes its resource to build the separated homogeneous embedded units (EU) and embed the secret information into EU. Then the attacker chooses attack strategies to destruct the secret information by destroying the attacked EU. The expected damage is evaluated by the case by the case when the attacker attacks a subset from all the EU. The expected damage that satisfy requirements: maximum damage in value from the point of view of the attacker and minimum from the embedder against the attacker, is the expected equilibrium damage. Based on the expected equilibrium damage, the optimal equilibrium capacity of deploying the secret information in the signal is calculated through the optimal number of EU with the embedded secret information (ESI). The embedder may deploy the secret information according to the limits of the optimal equilibrium capacity. And this algorithm will be more robust than methods without considering attack strategies.

This paper is organized as follows: section 2 discusses how to build the embedder-attacker system model based on the resource allocation of the embedder and the attacker. Section 3 mainly analyzes the influence of probability of correct detection of EU without ESI on the optimal equilibrium capacity of information hiding when the embedder embeds the secret information into the subset from EU and the attacker attacks the subset chosen from EU. Section 4 will give conclusion and future research of the discussion.

II. The Model

EU is the basic independent lowest-level unit into which the embedder writes λ bits binary information in the form of secret information. An example of EU is the independent components that are separated from the digital image using Fast Independent Component Analysis [15]-[16]. The embedder inserts the secret information into EU to conceal the secret

Ziquan Hu is with School of Computer Science and Engineering of University of Electronic Science and Technology of China (phone: 8618981912818; e-mail: ziquanhu@qq.com).

Kun She is with School of Computer Science and Engineering of University of Electronic Science and Technology of China (e-mail: kunshe@126.com).

Shahzad Ali is with School of Computer Science and Engineering of University of Electronic Science and Technology of China (e-mail: rsdcsiub@hotmail. com).

Kai Yan is with School of Computer Science and Engineering of University of Electronic Science and Technology of China (e-mail: yk@uestc.edu.cn).

information in the signal and ensure the effectiveness of EU and its secret information. It is assumed that the attacker can distinguish between EU with or without ESI. The attacker hopes to alter the secret information via modifying the value in the EU. Destructing any EU is to completely destroy the bit or all the bits in that EU only and functioning of remaining EU is not affected. Based on the information hiding, the embedder-attacker system consists of the embedder and the attacker. The embedder-attacker system has the following characteristics. All the EU are separated from each other so that when the attacker attacks the system, it only destroys merely EU with ESI and other EU remains safe. The embedder builds N EU, embeds the secret information into M out of N. ESI in the signal at least must meet user's demand. This relationship can be shown as

$$Mg \geq F, \tag{1}$$

where $M(M \leq N)$ is the number of EU with ESI, g is the performance factor of any EU in information hiding and F is user's demand. If ESI fails to satisfy user demand, it is futile to insert the secret information into the signal. When the number of destructing EU with ESI is less than $M - F/g$, the system still functions by ensuring the effectiveness of the remaining EU with ESI.

The entire resource r of the embedder is used to build EU and embed the secret information. The embedder must separate N EU from the digital signal. Let x be the average cost of building each EU. The embedder's resource must satisfy the requirement of building N EU as

$$r \geq Nx. \tag{2}$$

When the embedder embeds the secret information into N EU, the embedder's hiding capability per embedded EU t is

$$t = \frac{r - Nx}{M}. \tag{3}$$

The hiding capability is proportional to its resource. If the embedder has enough resources, then due to this, hiding capacity per EU is also high. According to (1-2), we can get

$$x \leq \frac{r}{\lceil F/g \rceil}. \tag{4}$$

The formula (4) shows that the upper bound of the average cost is determined by the resource of embedder, user's demand, and performance factor of each EU.

The vulnerability v [17]-[19] of each EU with ESI is

$$v = \frac{T^m}{T^m + t^m}, \tag{5}$$

where m is the contest intensity in the embedder-attacker system, T is the attacker's attacking force per attacked EU, and t is the embedder's hiding capability per embedded EU. If m=0 or 1, both the embedder and the attacker exerts the same influence on the vulnerability of each EU with ESI. If $0 < m < 1$, it gives a disproportional advantage of investing less than one's opponent. If $m > 1$, it gives a disproportional advantage of investing more resource than one's opponent.

Given the attacker distributes evenly its resource to $Q(1 \leq Q \leq N - h)$ undetected EU, there is a variable Q for the attacker to choose. The attacker's attacking force per attacked EU is

$$T = \frac{R}{Q}. \tag{6}$$

The attacking force from Q EU, which comprise M EU with ESI and $N - h - M$ EU without ESI, increases from $R/(N - h)$ to R. The probability that the attacker attacks f out of M is

$$\varphi(M, f) = \frac{\left(\begin{array}{c} M \\ f \end{array} \right) \left(\begin{array}{c} N - M - h \\ Q - f \end{array} \right)}{\left(\begin{array}{c} N - h \\ Q \end{array} \right)}, \tag{7}$$

where f varies from $\max\{0,\ Q - N + h + M,\ Q - s\}$ to $\min\{M,\ Q\}$. The attacker destroys h detected EU without ESI and $Q - f$ undetected EU without ESI from $N - h - M$ with probability 1, which almost consumes the attacker's resource. According to (3) and (5-6), the vulnerability of each EU from M EU with ESI is

$$v = \frac{1}{1 + \{(r - Nx)Q/(RM)\}^m}. \tag{8}$$

Given f out of M EU with ESI are attacked by the attacker, the probability of the attacker destructing k from f is

$$\phi(f, k) = \left(\begin{array}{c} f \\ k \end{array} \right) v^k\ (1 - v)^{f-k}, \tag{9}$$

where k=0, 1,..., f. The total number of destroyed EU is $k + Q - f$. Different k and f produce the same total number s of the destroyed EU when $k = s + f - Q$. The probability of destructing exactly s EU is

$$\begin{aligned} H_s(h, Q) = & \sum_{f=max\{0,Q-N+M+h,Q-s\}}^{min\{M,Q\}} \varphi(M, f)\phi(f, s + f - Q) \\ = & \left[\left(\begin{array}{c} N - h \\ Q \end{array} \right) \right]^{-1} \sum_{f=max\{0,Q-N+M+h,Q-s\}}^{min\{M,Q\}} \\ & \left(\begin{array}{c} f \\ s + f - Q \end{array} \right) \left(\begin{array}{c} M \\ f \end{array} \right) \left(\begin{array}{c} N - h - M \\ Q - f \end{array} \right) \times \\ & \frac{[(r - Nx)Q/(RM)]^{m(Q-s)}}{\{1 + [(r - Nx)Q/(RM)]\}^f}, \end{aligned} \tag{10}$$

where f from M EU with ESI and $Q - f$ out of $N - h - M$ EU without ESI are attacked, and h is the number of the detected EU without ESI. The expected damage caused by the attacker who chooses different attack strategies Q is

$$d(h, Q) = \sum_{s=0}^{Q} H_s\ max\{0, F - g(N - h - s)\}. \tag{11}$$

The expected damage to the embedder-attacker system is

$$Damage(N, M) = \sum_{h=0}^{N-M} \pi(h)\ d(h, Q^*), \tag{12}$$

where $\pi(h)$ is

$$\pi(h) = \left(\begin{array}{c} N - M \\ h \end{array} \right) q^h\ (1 - q)^{N-M-h}, \tag{13}$$

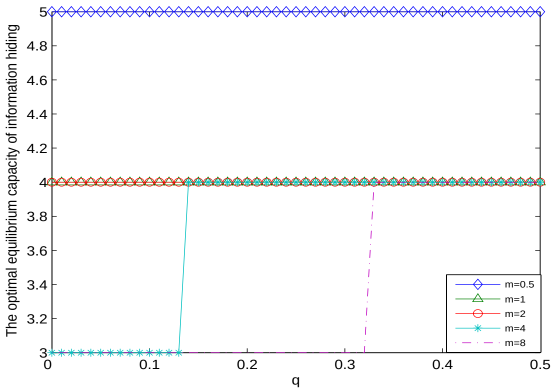

Fig. 1. The optimal equilibrium capacity of information hiding for r =8, R=2, F=6, g=2, λ=1, x=1.2.

where q is the probability of correct detection of EU without ESI. Q^* is formulated as

$$Q^* = \arg \underset{Q}{max}\ d(h,Q). \tag{14}$$

There is a free variable Q chosen by the attacker that maximizes $d(h,Q)$.

$$(N^*,M^*) = \arg \underset{N\ ,\ M}{max}\ Damage(N,M). \tag{15}$$

When N=N^* and M=M^*, $Damage(N,M)$ is equal to the expected equilibrium damage D.

Therefore, the optimal equilibrium capacity of the secret information is

$$C^* = \lambda\ M^*, \tag{16}$$

where λ is the number of binary information per embedded EU with ESI.

According to (2), N is limited, M^* and Q^* are limited. There must exist Nash Equilibrium M^* and Q^*. The optimal equilibrium capacity of information hiding in the signal is calculated by applying the enumerative algorithm as follows:

Algorithm 1:

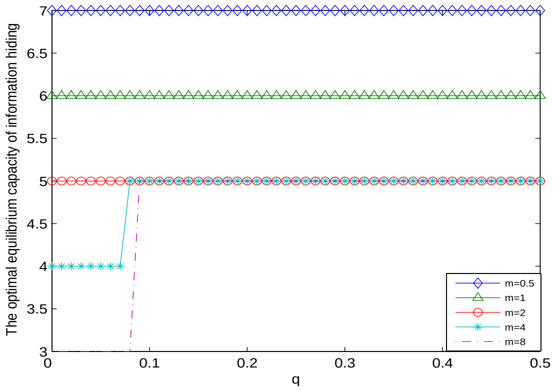

Fig. 2. The optimal equilibrium capacity of information hiding for r =8, R=2, F=6, g=2, λ=1, x=0.9.

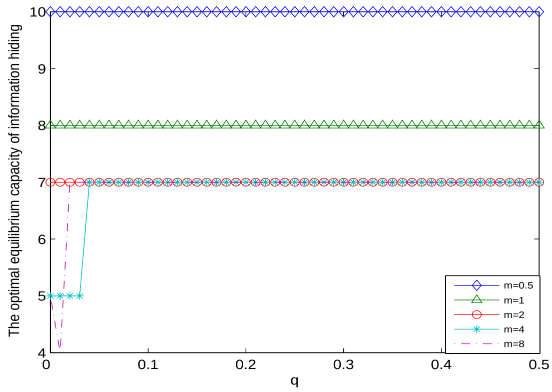

Fig. 3. The optimal equilibrium capacity of information hiding for r =8, R=2, F=6, g=2, λ=1, x=0.6.

```
Input: $r$, $R$, $F$, $g$, $\lambda$, $x$
Output: $N^*$, $M^*$, $Q^*$, $C^*$, $D$
for $N$=1,..., $N_{max}$($N_{max}$ is $\lceil r/x \rceil$)
    for $h$=0,..., $N-M$
        dmax=0;
        for $s$=1,..., $Q$
            if $F-g(N-h-s) \leq 0$ then
                $H_s$=0;
            else
                Use (10) to compute $H_s$;
            end if
            Calculate $d(h,Q)$, applying (11);
        end for $s$
            if $d(h,Q)$ >dmax then
                dmax =$d(h,Q)$;
            end if
            Compute $Q^*$ according to (14);
            Calculate $D(N,M)$, according to (12);
    end for $h$
    Calculate the optimal values $N^*$ and $M^*$, using (15);
    Applying (16) compute the optimal equilibrium capacity;
end for $N$.
```

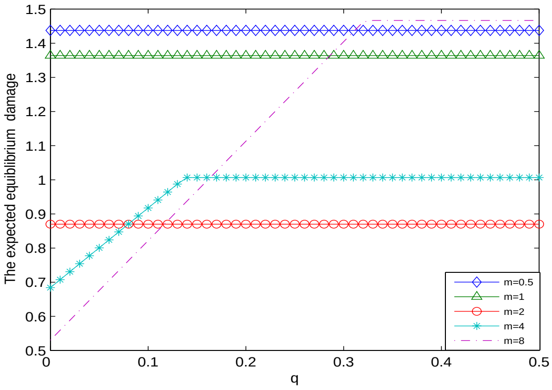

Fig. 4. The expected equilibrium damage for r =8, R=2, F=6, g=2, λ=1, x=1.2.

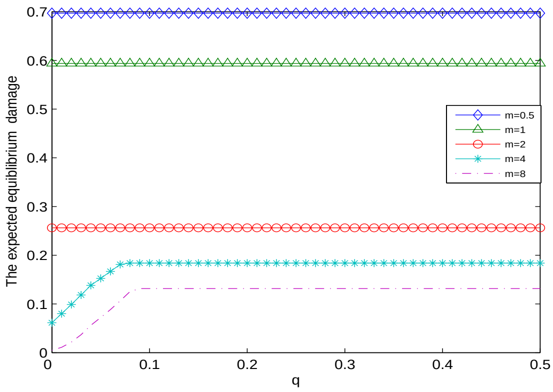

Fig. 5. The expected equilibrium damage for r =8, R=2, F=6, g=2, λ=1, x=0.9.

III. Analysis of the Model

Figures 1-9 present optimal equilibrium capacity C^* of information hiding, the optimal number of building EU, and the expected equilibrium damage D as functions of x and m for r=8, R=2, F=6, g=2, λ=1. Since λ=1, according to (15), $C^* = M^*$. With performance factor g=2 for inserting the secret information into each EU, the embedder must embed at least M=3 EU to meet user's demand F=6 according to (1). Therefore M^* <3 is never an optimal value. Allocating resource r=8 to $N \geq 3(M \leq N)$ EU means maximum cost of building each EU is r/N=2.67. Hence if the cost x exceeds 2.67, the embedder embeds the secret information into EU that can't meet user's demand when no attacks occur. It can be seen that the optimal number C^* of EU with ESI for the cost x =1.2, 0.9, 0.6 of building each EU is presented in figure 1, 2, 3 respectively. It is observed that C^* is insensitive to q or increases monotonically with q, except that for high contest (m=4 or 8), low q and x=0.6, C^* deceases firstly.

When the cost of building each EU deceases from x=1.2 to 0.6, the optimal value C^* increases from 3 to 10 since the less resources in building the EU, the more remaining EU of the embedder's resource is used to embed the secret information into EU. The more intensive contest is, the less C^* gets, because the higher contest consumes the more resource of the embedder to increase the hiding capability per embedded EU and protect the secret information in EU. We can see that the expected equilibrium damage D for the cost x =1.2, 0.9, 0.6 of establishing EU is described in figure 4, 5, 6 respectively. The damage remains unchanged or increases with q. It can be analyzed as follows: the number of building EU is equal to that of the EU with ESI (figures 1, 2, 3, 7, 8, 9), therefore there aren't EU without ESI. The reduction of the average cost in building EU can insert more secret information into EU, protect more EU with ESI, and hence the damage almost decreases to 0 when cost x is low.

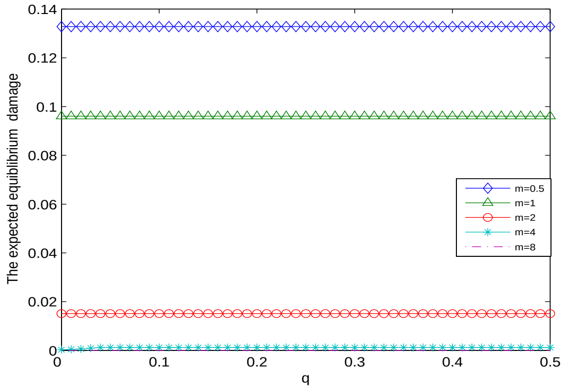

Fig. 6. The expected equilibrium damage for r =8, R=2, F=6, g=2, λ=1, x=0.6.

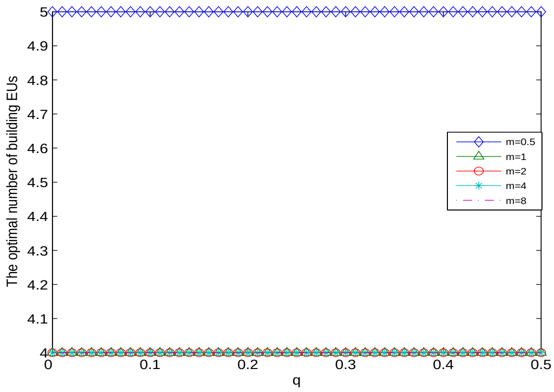

Fig. 7. The optimal number of building EU for r =8, R=2, F=6, g=2, λ=1, x=1.2.

IV. Conclusion

In this work, we discussed the optimal number of EU with ESI in the signal by allocating the resource of the embedder between two main actions: building separated EU from the digital signal, and embedding the secret information into EU. It is supposed that the embedder builds the embedder-attacker

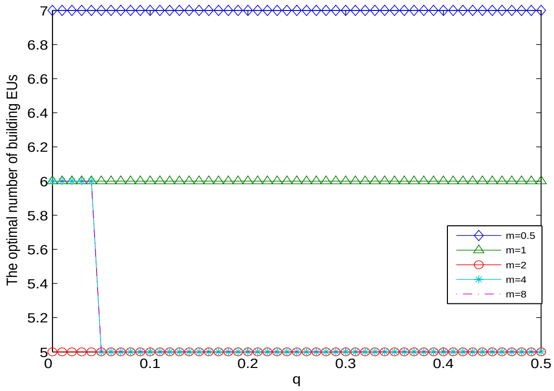

Fig. 8. The optimal number of building EU for r =8, R=2, F=6, g=2, λ=1, x=0.9.

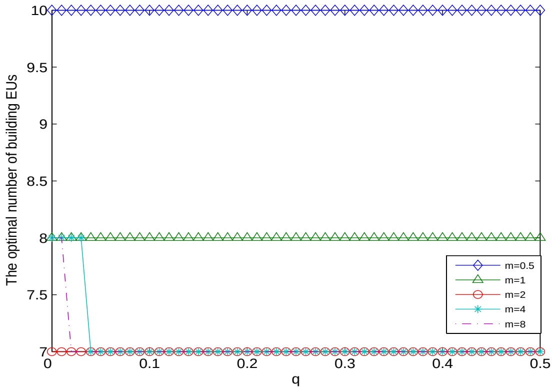

Fig. 9. The optimal number of building EU for r =8, R=2, F=6, g=2, λ=1, x=0.6.

system first. Then the attacker chooses its attack strategies to attack the system. The attacker can explore all the EU and try to detect the EU without ESI. All the detected EU without ESI are destroyed without consuming of the attacker's resource. Then the attacker allocates its resource evenly to the undetected EU. The paper analyzes the influence of the probability q of correct detection of EU without ESI on the optimal equilibrium capacity, and on the expected equilibrium damage when the embedder-attacker system is balanced. It is shown that the optimal equilibrium capacity is either insensitive to q or increases with the growth of q. With q is lower, the embedder may establish EU and deploy the secret information into all the EU and not necessarily leave EU without ESI. The higher probability of the attacker to correct detection makes it important for the embedder to embed less secret information into EU. The decrease of the contest intensity makes the optimal number of EU with ESI more insensitive to q; in this case the embedder may insert the secret information into all the EU. And last but not least, since the number of building EU equals to the number of EU with ESI, the expected equilibrium damage is insensitive to q.

In our future work, we are planning to consider the equilibrium capacity of information hiding when the embedder-attacker system is attacked by unintentional and intentional impacts.

Acknowledgment

The authors thank the anonymous referees for their useful comments.

References

[1] Elias K., Saraju P. M., *et al*, Hardware assisted watermarking for multimedia, Computers and electrical engineering, vol.35, no.2, 2009, pp. 339-358.

[2] M. Fan, H. Wang, Chaos-based discrete fractional sine transform domain audio watermarking scheme, Computers and electrical engineering, vol. 35, no. 3, pp. 2009, 506-516.

[3] Hazem A. A., Allam O. A., Adaptive color image watermarking based on a modified improved pixel-wise masking technique, Computers and electrical engineering, vol. 35, no. 5, 2009, pp. 673-695.

[4] A. Kaneda, Y. Fujii *et al*, An Improvement of Robustness Against Physical Attacks and Equipment Independence in Information Hiding Based on the Artificial Fiber Pattern, 2010 International Conference on Availability, Reliability and Security, 2010, pp. 608-612.

[5] M. E. Andrés, C. Palamidessi *et al*, Computing the Leakage of Information-Hiding Systems, Lecture Notes in Computer Science,Springer Berlin/Heidelberg, 2010, pp. 373-389.

[6] Cooperman M, Moskowitz S, Steganographic method and device, USA: patent, 1997.

[7] Q. Li, I. J. Cox, Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking, IEEE transaction on information forensics and security, vol. 2 no. 2, 2007, pp. 127-139.

[8] L. M. Marvel, C. G. Boncelet Jr., C. T. Retter, Spread spectrum image steganography, IEEE Transaction on image processing, vol. 8, no. 8, 1999, pp. 1075-1083.

[9] W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, Tech. Rep., MIT media Lab, 1994.

[10] S. Pereira, T. Pun, Fast robust template matching for affine resistant image watermarks, http://cuiwww.unige.ch/vision, 1999.

[11] T. Aura, Practical invisibility in digital communication. Springer Berlin/Heidelberg, 1996, pp. 265-278.

[12] G. Levitin, K. Hausken, Influence of attacker's target recognition ability on defense strategy in homogeneous systems, Reliability Engineering and System Safety, vol. 95, 2010, pp. 565-572.

[13] G. Levitin, K. Hausken, Protection vs. redundancy in homogeneous parallel systems, Reliability Engineering and System Safety, vol. 93, 2008, pp. 1444-1451.

[14] G. Levitin, K. Hausken, Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts, IEEE transactions on reliability, vol. 58, no. 4, 2009, pp. 679-690.

[15] F. Kahl, S. Agarwal *et al*, Practical global optimization for multiview geometry, Int J Comput Vis, vol. 79, no. 3, 2008, pp. 271-284.

[16] Hyvärinen, Fast and robust fixed-point algorithms for independent component analysis, IEEE Transactions on Neural Networks, vol. 10, no. 3, 1999, pp. 626-634.

[17] Skeperdas S, Contest success functions, Economic theory, 1996 90-283.

[18] Tullock G, Efficient rent-seeking, In: Buchnana JM, Tollison RD, Tullock G, editors, Toward a theory of the rent-seeking society, College station:Texas A&M university press, 1980, 97-112.

[19] Hausken K, Production and conflict models versus rent seeking models, Public choice 2005, 123:59-93.

Ziquan Hu was born in Chongqing, China, in 1976. He received his bachelor degree from College of Computer and Information Science, Chongqing Normal University in 2001, and master degree from Department of Computer Science and Technology, Chongqing University of Posts and Communications in 2006 respectively. He is currently Ph.D candidate in School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC). His research interests include Signal processing, game theory and information hiding.

Kun She is Ph.D, Professor of School of Computer Science and Engineering in UESTC. His research interests covers Wavelet analysis, MiddleWare and Information security.

Shahzad Ali is Ph.D. candidate in the Graduate School of Computer Science and Engineering, UESTC, Chengdu, China. His research interests include energy efficient cloud computing, game theoretical approach for resource allocation in cloud data centers.

Kai Yan is Ph.D candidate in School of Computer Science and Engineering of UESTC. She received her master degree from School of Communication and Information Engineering of UESTC. Her research interests include network communication, game theory and Rough set.