

# Analysis of Information Hiding Based on False Objects versus Attack Strategies

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

*Abstract*—There are false objects in the information hiding field. The embedder can deploy false objects into digital signal to increase the hiding capability per embedded unit, protect its embedded secret information and minimize the expected damage, while the attacker hopes to maximize it. In this paper, 2-phase game can be applied to build the embedder-attacker system to analyze this conflicted issue. In the system, the embedder consumes its resource to build embedded units (EU) and insert secret information or false objects into EU. The attacker distributes its resource evenly to the attacked EU. The expected equilibrium damage, which is maximum damage in value from the point of the view of the attacker and minimum from the embedder, is evaluated by 2-phase game theory. Finally, compute the expected equilibrium damage, the optimal number of building EU and the optimal number of EU with the embedded secret information (ESI). The optimal equilibrium capacity of hiding information on the basis of false objects and attack strategies is calculated through the optimal number of EU with ESI.

*Keywords*—2-Phase Game, Attack Strategies, Expected Equilibrium damage, False Objects, Information Hiding, Optimal Equilibrium Capacity.

## I. INTRODUCTION

**I**N the information hiding technique, first we embed the secret information into the digital signal such as audio, image and video, and pass the secret information through the open channel. Robustness, undetectability and capacity are three most important factors of information hiding [1]-[5]. There are lots of important methods proposed by the researchers increasing robustness of information hiding. 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

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: rsdc-siub@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).

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 in the signal when the attacker has options of attack strategies? How to deploy the false objects to resist the malicious impact of the attacker? 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 resolved 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 attacking EU. The expected damage is evaluated by the case when the expected equilibrium damage (maximum damage in value from the point of view of the attacker and minimum from the embedder against the attacker) is reached. Therefore the optimal equilibrium capacity of deploying the secret information into the signal is calculated through the optimal number of EU with the embedded secret information (ESI). These methods applying the fundamental limits of the optimal equilibrium capacity will be more robust, compared with those without considering attack strategies, because the embedder may deploy the secret information on the basis of the guiding result of this paper.

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 the probability of the detected EU with embedded false objects on the optimal equilibrium capacity of information hiding when the embedder embeds the secret information or false objects into the subset from all the EU, and the attacker attacks the subset chosen from EU. Section 4 will give conclusion and future research of the discussion.

## II. THE EMBEDDER-ATTACKER SYSTEM MODEL

EU is the basic independent lowest-level unit in which the embedder writes  $\lambda$  bits binary information in the form of secret information. An example of EU is the independent components that are separated from the original image using Fast

Independent Component Analysis [15]-[16]. The embedder inserts the secret information or false objects (FO) into EU to conceal the secret information in the signal and ensure the effectiveness of EU and their secret information. It is assumed that the attacker can distinguish EU with ESI from one with FO. The attacker hopes to destruct the secret information by altering the value in the attacked 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 separate so that when it attacks the system, the attacker merely destroys a single EU and its ESI, but can't have the impact on others. The embedder builds  $N$  EU, embeds the secret information into  $M$  out of  $N$ . ESI in the signal at least must meet user 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 demand. If ESI fails to satisfy user demand, it is futile to insert the secret information into the signal. When the number of destructed EU with ESI is less than  $M - \lceil F/g \rceil$ , the system still functions by ensuring the effectiveness of the remaining EU with ESI. The entire resource  $r$  of the embedder is used to establish the EU and embed the secret information or FO into EU. The embedder must separate  $N$  EU from the signal. Let  $x$  be the average cost of building each EU. The embedder's resource must satisfy the requirement of building  $N$  EU as

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

The embedder embeds the secret information into  $M$  EU, inserts FO into  $N - M$  EU. Let  $y$  be the cost of inserting each FO. The embedder's hiding capability per embedded EU  $t$  is

$$t = \frac{r - Nx - (N - M)y}{M}. \tag{3}$$

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 of constructing  $N$  EU is determined by the embedder's resource, user 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 effort than one's opponent. Let

$h$  be the number of the detected EU with the embedded FO (EFO). Given the attacker distributes evenly its resource to  $Q$  ( $1 \leq Q \leq N - h$ ) detected EU, there is a variable  $Q$  for the attacker to choose. The attacker's attacking force per attacked EU is

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

It is supposed that the attacker can explore all the EU and try to detect EU with EFO. All the detected EU with EFO are destroyed without any cost of the attacker's resource, because the target of the attacker's destructing is EU with ESI, not ones with EFO, and because the attacker will avoid attacking the detected EU with EFO. Then the attacker distributes its resource evenly to the undetected EU. The attacker's attacking force per attacked EU from  $Q$  EU, which comprise  $M$  EU with ESI and  $N - h - M$  EU with EFO, increases from  $R/(N - h)$  to  $R$ . The probability that the attacker attacks  $f$  out of  $M$  is

$$\delta(M, f) = \frac{\binom{M}{f} \binom{N - M - h}{Q - f}}{\binom{N - h}{Q}}, \tag{7}$$

where  $f$  varies from  $\max \{0, Q - N + M + h, Q - s\}$  to  $\min \{M, Q\}$ . The attacker destroys  $h$  detected EU with EFO, and  $Q - f$  undetected EU with EFO from  $N - M - h$  with probability  $b$ , which almost doesn't consume any resource. The vulnerability of each EU from  $M$  EU with ESI is

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

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

$$\begin{aligned} \beta(f, k) &= \binom{f}{k} v^k (1 - v)^{f-k} \\ &= \binom{f}{k} \frac{[(r - Nx - (N - M)y)Q/(RM)]^{m(f-k)}}{\{1 + [r - Nx - (N - M)y]Q/(RM)\}^f}, \end{aligned} \tag{9}$$

where  $k = 0, 1 \dots f$ . The probability of destructing  $j$  ( $j=0 \dots Q - f$ ) out of  $Q$ -s EU with EFO is

$$\gamma(Q - f, j) = \binom{Q - f}{j} b^j (1 - b)^{Q-f-j}. \tag{10}$$

where  $b$  is the probability of destructing EFO. The total number of the destroyed EU is  $k + s$ . Different  $k$  and  $f$  produce the same total number  $s$  of the destroyed EU when  $j = s - k$ . The probability of destructing exactly  $s$  EU is

$$\begin{aligned} H_s(h, Q) &= \sum_{f=\max\{0, Q-N+M+h, Q-s\}}^{\min\{M, Q\}} \delta(M, f) \times \\ &\sum_{k=0}^f \beta(f, k) \sum_{j=0}^{Q-f} \gamma(Q - f, j), \end{aligned} \tag{11}$$

where  $j = s - k$ ,  $f$  from  $M$  EU with ESI and  $Q - f$  out of  $N - h - M$  EU with EFO are attacked, and  $h$  is the number of the detected EU with EFO. The expected damage caused by the attacker who chooses different attack strategies  $Q$  is

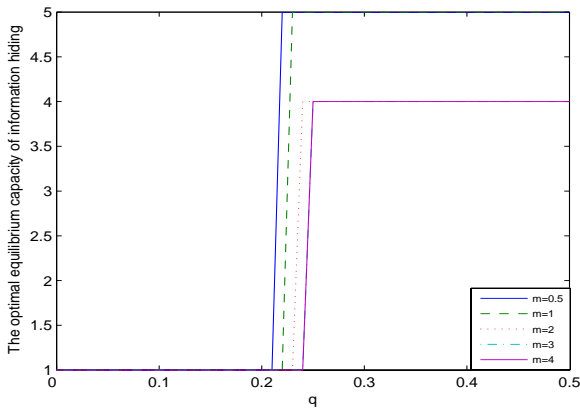


Fig. 1. The optimal equilibrium capacity of information hiding for  $r=10$ ,  $R=2$ ,  $F=6$ ,  $g=2$ ,  $\lambda=1$ ,  $b=0.5$ ,  $x=1$ ,  $y=0.3$ .

$$d(h, Q) = \sum_{s=0}^Q H_s \max\{0, F - g(N - h - s)\}. \quad (12)$$

The expected damage to the embedder-attacker system is

$$Damage(N, M) = \sum_{h=0}^{N-M} \pi(h) d(h, Q^*). \quad (13)$$

In (13),  $\pi(h)$  is

$$\pi(h) = \binom{N-M}{h} q^h (1-q)^{N-M-h}. \quad (14)$$

There is a free variable  $Q$  chosen by the attacker that maximizes  $d(h, Q)$ . In (13),  $Q^*$  is formulated as

$$Q^* = \arg \max_Q d(h, Q). \quad (15)$$

When the embedder minimizes the expected damage, a couple of parameters are

$$(N^*, M^*) = \arg \max_{N, M} Damage(N, M). \quad (16)$$

Therefore, the optimal equilibrium capacity of the secret

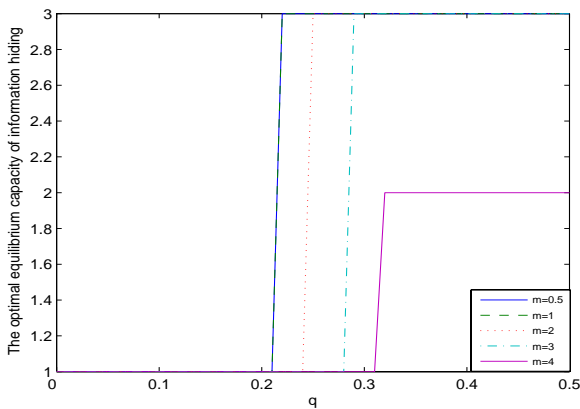


Fig. 2. The optimal equilibrium capacity of information hiding for  $r=10$ ,  $R=2$ ,  $F=6$ ,  $g=2$ ,  $\lambda=1$ ,  $b=0.5$ ,  $x=2$ ,  $y=0.3$ .

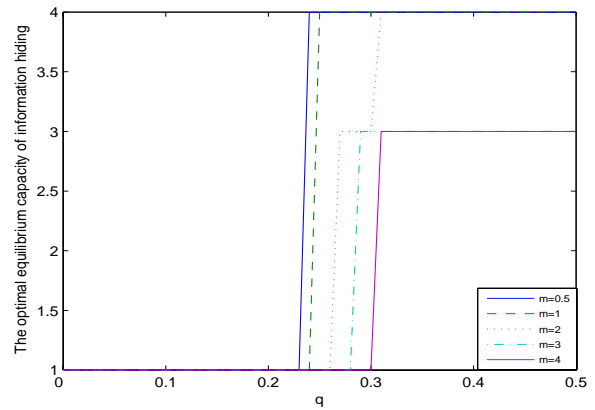


Fig. 3. The optimal equilibrium capacity of information hiding for  $r=10$ ,  $R=2$ ,  $F=6$ ,  $g=2$ ,  $\lambda=1$ ,  $b=0.5$ ,  $x=1$ ,  $y=0.5$ .

information is

$$C^* = \lambda M^*, \quad (17)$$

where  $\lambda$  is the number of binary information per EU with ESI. The embedder's resource  $r$  is used to build  $N$  EU and insert the secret information and FO into  $M$  and  $N - M$  EU respectively, so  $r - Nx - (N - M)y \geq 0$ ,  $r - N(x + y) > 0$ ,  $N < \lceil r/(x + y) \rceil$ . There must exist Nash Equilibrium  $(M^*, N^*)$  in the information hiding.  $M^*$ ,  $N^*$ ,  $C^*$  and the expected equilibrium damage are calculated by applying the enumerative algorithm as follows:

```

for  $N=1, \dots, N_{max}$  ( $N_{max}$  is  $\lceil r/(x + y) \rceil$ )
  for  $h=0, \dots, N - M$ 
    dmax=0;
    for  $s=1, \dots, Q$ 
      if  $F - g(N - h - s) \leq 0$  then
         $H_s=0$ ;
      else
        Use (11) to compute  $H_s$ ;
      end if
      Calculate  $d(h, Q)$ , applying (12);
  
```

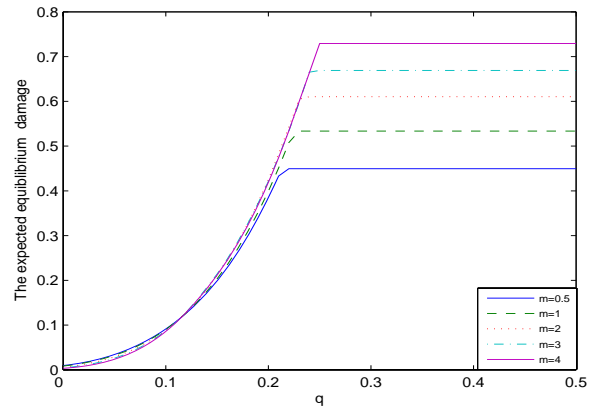


Fig. 4. The expected equilibrium damage to the embedder-attacker system for  $r=10$ ,  $R=2$ ,  $F=6$ ,  $g=2$ ,  $\lambda=1$ ,  $b=0.5$ ,  $x=1$ ,  $y=0.3$ .

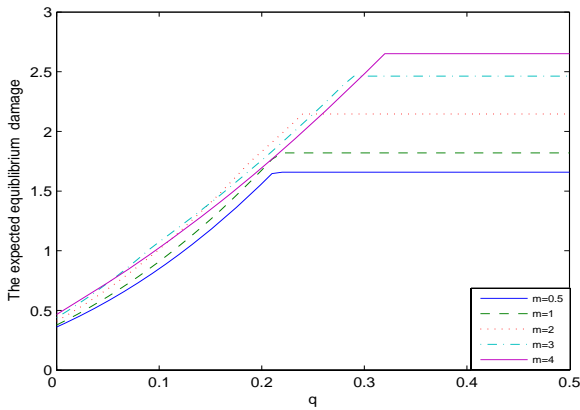


Fig. 5. The expected equilibrium damage to the embedder-attacker system for  $r=10, R=2, F=6, g=2, \lambda=1, b=0.5, x=2, y=0.3$ .

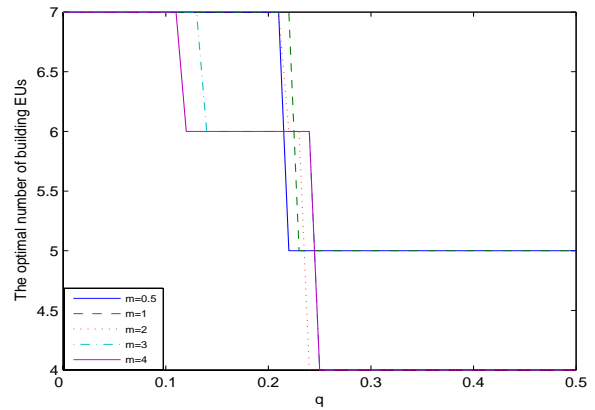


Fig. 7. The optimal number of building EU for  $r=10, R=2, F=6, g=2, \lambda=1, b=0.5, x=1, y=0.3$ .

```

end for s
if  $d(h, Q) > d_{max}$  then
     $d_{max} = d(h, Q)$ ;
end if
Compute  $Q^*$  according to (15);
Calculate  $D(N, M)$ , according to (13);
end for h
Calculate the optimal values  $N^*$  and  $M^*$ , using (16);
Applying (17) compute the optimal equilibrium capacity;
end for  $N$ .
    
```

### III. ANALYSIS OF THE MODEL

Figures 1-9 present the optimal value of constructing EU, optimal equilibrium capacity  $C^*$  of information hiding, and the expected equilibrium damage  $D$  as functions of  $x, y$  and  $m$  for  $r=10, R=2, F=6, g=2, \lambda=1, b=0.5$ . Since  $\lambda=1$ , according to (17),  $C^* = M^*$ . With performance factor  $g=2$  for inserting the secret information into each EU, the embedder must embed at least  $M=3$  EU to meet the user demand  $F=6$  according to (1). Therefore  $M^* < 3$  is never an optimal value. Allocating resource  $r=10$  to  $N \geq 3(M \leq N)$  EU means maximum cost

of building each EU is  $r/N=3.33$ . Hence if the cost  $x$  exceeds 3.33, the embedder embeds the secret information into EU, which doesn't meet the user demand when no attacks occur.

It can be seen that the optimal number  $C^*$  of  $(x, y) = (1, 0.3), (2, 0.3), (1, 0.5)$  of building each EU is presented in the figure 1, 2, 3 respectively. It is observed that  $C^*$  is insensitive to  $q$  or increases monotonically with  $q$ . When the cost of establishing each EU decreases from  $x=2$  to 1, the optimal value  $C^*$  increases from 3 to 5 since the less resource in building the EU, the more remaining EU of the embedder's resource is used in embedding the secret information into EU. When the cost of embedding FO decreases from 0.5 to 0.3,  $C^*$  increases from 4 to 5. The more intensive contest is, the less  $M^*$  gets, because the higher contest between the embedder and the attacker consumes more embedder's resource 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  $(x, y) = (1, 0.3), (2, 0.3), (1, 0.5)$  of establishing EU is described in the figure 4, 5, 6 respectively. The damage remains unchanged or increases with  $q$ . It can be analyzed

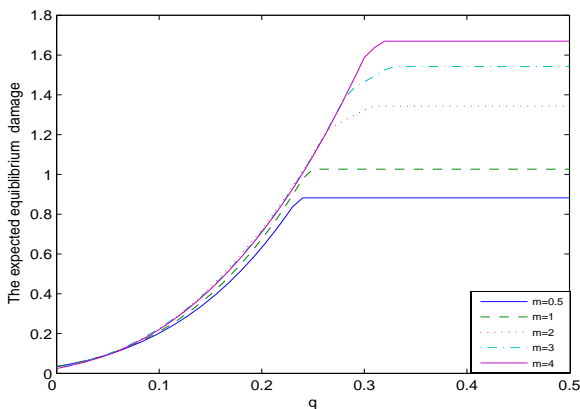


Fig. 6. The expected equilibrium damage to the embedder-attacker system for  $r=10, R=2, F=6, g=2, \lambda=1, b=0.5, x=1, y=0.5$ .

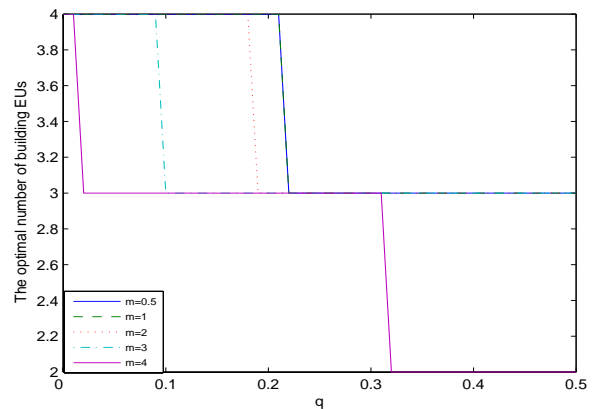


Fig. 8. The optimal number of building EU for  $r=10, R=2, F=6, g=2, \lambda=1, b=0.5, x=2, y=0.3$ .

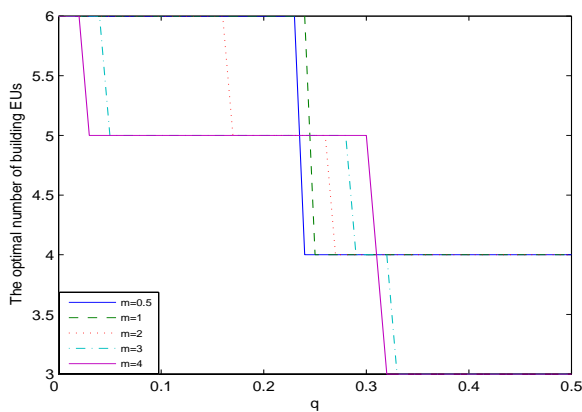


Fig. 9. The optimal number of building EU for  $r=10$ ,  $R=2$ ,  $F=6$ ,  $g=2$ ,  $\lambda=1$ ,  $b=0.5$ ,  $x=1$ ,  $y=0.5$ .

as follows: the number of building EU is equal to that of the embedded EU (see also figures 1-3, 7-9), therefore there are not EU with EFO. The reduction of the average cost in constructing EU enables the embedder to insert more secret information into EU, protect more EU with ESI, and hence the damage almost decreases to 0 when cost  $x$  is low.

#### 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 the separated EU from the original signal, and embedding the secret information or FO into EU. It is supposed that the embedder builds the embedder-attacker system first. The attacker chooses its attack strategies to attack the system. It can explore all the EU and try to detect EU with EFO. All the detected EU with EFO are destroyed with negligible effort. Then the attacker allocates its resource evenly to the undetected EU. This paper analyzes the influence of probability  $q$  of detected EU with EFO on the optimal number of building EU, on the optimal number of EU with 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 number of EU with ESI is either insensitive to  $q$  or increases with the growth  $q$ . With  $q$  is lower, the embedder may build EU and deploy the secret information into all the EU and not necessarily insert FO into EU. The higher probability of correct detection for the attacker makes it important for the embedder to embed less secret information into EU. Since the number of building EU is that of embedded EU, the expected equilibrium damage is insensitive to  $q$ . The decrease of the contest intensity makes the optimal number of EU with ESI less insensitive to  $q$ , therefore in the case the embedder inserts the secret information into all the EU. The optimal number of EU with ESI determines the optimal equilibrium capacity of information hiding based on FO.

In our future work, we are planning to consider the equilibrium capacity of information hiding based on false objects

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: Buchana 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.