Performance Comparative of Data Embedding Rules in Watermarking

Jin Cong
Department of Computer Science, Central China Normal University, Wuhan 430079, P.R. China

Abstract
Though image data hiding (Digital watermarking) as a tool for copyright protection is quite recent, a great deal of research has been carried out mainly addressing the development of robust, yet unperceivable, watermarking strategies. As it is now becoming evident, however, other important issues have to be analyzed in order to make watermark-based copyright protection feasible. Among them, the analysis and comparison of the performance of additive embedding rule, multiplicative embedding rule and fusion embedding rule plays a mayor role. In this paper, the watermarking is assumed to consist in the modification of a set of full-frame DCT coefficients. The watermark channel is modeled by letting the watermark be the signal and the original image DCT coefficients the noise introduced by the channel. To derive the capacity of each coefficient, the channel transition matrix is computed. An evaluation of the number of bits that can be hidden within a digital image by means of DCT domain watermarking is given. These calculated results are derived by using three embedding rules, respectively. Experimental results show that different performance of three kinds of embedding rules, these performance have offered basis on which we use these embedding rules rationally.

Keywords: *Image Hiding; Embedding Rule; Copyright Protection; Channel Capacity*

1 Introduction

The last decade has experienced a rapid evolution in multimedia storage and transmission technology. Part of this evolution was the development of the field of multimedia security and copyright protection. The field emerged because of the growing concern about the ease of copying and reproducing data sources in a digital format. This can increase the chance of theft and piracy of intellectual property. Researchers have proposed the use of digital watermarking as a means of copyright protection and data authentication [1,2]. Furthermore, there are other applications related to security, such as transmitting information between two or more parties using what is known as subliminal channels [3], where information between two or more parties is exchanged in an innocuous way through a public communication channel. In some multimedia applications, encrypting a message does not provide enough security, and the message's very existence needs to be concealed. This is of form of digital steganography.

Steganography is about concealing their very existence. It is usually interpreted to mean hiding information in other information. There are many steganography techniques that can be found in the literature. For an overview of the basic techniques one can consult [4]. Image hiding techniques are one of the steganographies which hides a secret image or a confidential image, for instance, a military map, in a original image and thus creates a camouflage image [5]. The technique should be capable of hiding the secret image in the original image with several limits [6]. A fundamental requirement of an image hiding system is that not only should the original image be no-objectively degraded, but the secret image should also be minimally perceptible.

Though image data hiding (Digital watermarking) as a tool for copyright protection is quite recent, a great deal of research has been carried out mainly addressing the development of robust, yet unperceivable, watermarking strategies. As it is now becoming evident, however, other important issues have to be analyzed in order to make watermark-based copyright protection feasible. Among them, the analysis and comparison of the performance of additive embedding rule, multiplicative embedding rule and fusion embedding rule plays a mayor role.

In this paper, we introduce existing image data embedding rule briefly at first, these image embed

rules already got extensive application in the practical problem. Among these embedding rules, additive embedding rule, multiplicative embedding rule and fusion embedding rule are the most frequently used. But, what differences does the performance of these three kinds of embedding rules have? Which kind of embedding rule is better? These questions nobody study even so far, but these questions are very important. So necessary to carry on deep analysis and study to these questions. In this paper, the watermarking is assumed to consist in the modification of a set of full-frame DCT coefficients. The watermark channel is modeled by letting the watermark be the signal and the original image DCT coefficients the noise introduced by the channel. To derive the capacity of each coefficient, the channel transition matrix is computed. An evaluation of the number of bits that can be hidden within an digital image by means of DCT domain watermarking is given. These calculated results are derived by using three embed rules, respectively. Through analyses and compare, we will give such conclusion: which embedding rule is better under some conditions.
The remainder of this paper is organized as follows. In section 2, we introduce three kinds of image data embedding rules. In section 3, watermark channel modeling and its statistical characteristics are discussed. In section 4, estimation on test data is discussed. Experimental results are reported in section 5. Conclusions are presented in section 6.

2 Digital Image Hiding Models

An important issue in digital image hiding is a camouflage image should only be an imperceptible modification of the original image, but at the same the secret image can be extracted. To be able to have practical image hiding schemes, it is of eminent importance to have good extraction schemes available. We do not discuss extraction problem in detail as they are beyond the scope of this paper.

In the literature it is very common that the secret image is hidden in an additive embedding rule (see [7]), i.e.,

(rule 1) $$v_i' = v_i + \alpha w_i$$

where $\{v_i\}$ denotes the original image DCT coefficient, $\{v'_i\}$ is the camouflage image coefficient, $\{w_i\}$ is the secret image coefficient, i is i-th component, and α is the strength factor controlling the watermarking strength.

Another different way of the hiding secret image is multiplicative embedding rule. The camouflage image data v'_i are now formed from the secret image data w_i and the original image data v_i according to

(rule 2) $$v_i' = v_i(1 + \alpha w_i)$$

This way of hiding image was proposed, among others, by Cox et.al.[8]. According this embedding rule, watermark embedding is achieved by modifying a set of full-frame DCT coefficients of the image.

In recent years, the fusion embedding rule get extensive concern, its embedding rule is

(rule 3) $$v_i' = (1-\alpha)v_i + \alpha w_i, \quad 0 \le \alpha < 1$$

This rule can be defined as the process by the some features of original image and secret image, are fused together to form a camouflage image.

How are the performance using embedding rule 1, 2, and 3 for hiding a secret image? What superiority is there compared with anther two rules? We will answer these questions by the experiments in section 5.

3. Watermark Channel Modeling and Its Statistical Characteristics

A lot of scientists study the image data hiding question using information theory[9-12]. According to Smith and Comiskey[13] and Servetto et al[14], the watermark channel is modeled as an AWGN channel, so that the corresponding popular capacity theorem[9] can be used. Such an analysis, however, only applies to cases where the watermark is simply added to a set of features extracted from the original image data. Besides, the features the watermark is added to must be such that they can be modeled as Gaussian random variables. As a matter of fact, the embedding rule is only rarely additive, and the Gaussian approximation is not verified in most practical cases.

According to Kalker et al.[15], the probability distribution of the secret image coefficients does not

have a significant impact on secret image decoding reliability. Barni et al. have proposed a watermark channel modeling in [16]. They think that the secret image coefficient w_i to the to-be-transmitted signal, the camouflage image coefficient v'_i to the channel output, and the original image coefficient v_i to the channel noise. Obviously, the additive Gaussian noise assumption does not hold, even by neglecting the presence of attacks. Indeed the noise does not follow a Gaussian probability density function (pdf), since DCT coefficient can't be modeled as Gaussian random variable.

Let $p_{v_i}(v)$ denote the pdf of the random variable v_i. It is assumed that v_i's are independent identically distributed, i.i.d., variables. Therefore, hereafter the index i will be overlooked. Since the Gaussian assumption is inaccurate for DCT coefficients of original images, some authors have proposed the generalized Gaussian probability density function

$$p_x(x) = Ae^{-|\beta x|^c} \qquad (*)$$

as an alternative leading to improved statistical models [17]. Note that the Gaussian and the Laplacian pdf's are just special cases of this expression, given by c=2 and c=1, respectively.

The parameters A and β in equation (*) can be expressed as

$$\beta = \frac{1}{\sigma}\sqrt{\frac{\Gamma(3/c)}{\Gamma(1/c)}}; \qquad A = \frac{\beta c}{2\Gamma(1/c)}; \qquad \Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx,$$

where σ is the standard deviation. Hence, the pdf is completely specified by c and σ. The shape of the $p_x(x)$ for various shape parameters is depicted in figure 1.

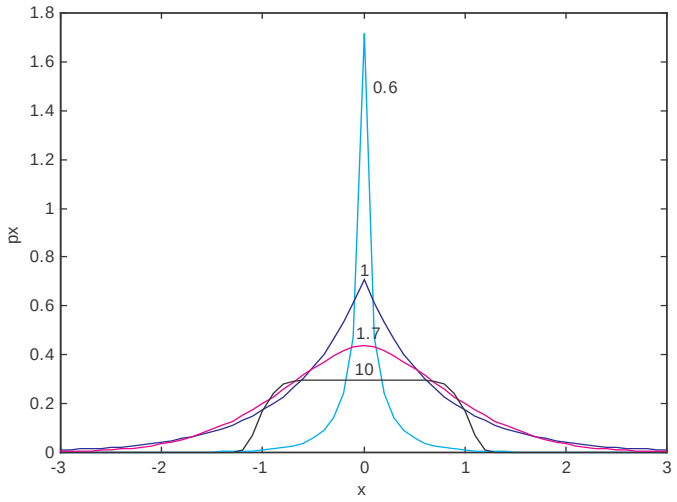

Figure 1. *Shape of the generalized Gaussian distribution for various c*=0.6, 1, 1.7, *and* 10, *where* σ =1.

By equation (*), $p_{v'}(v'|w)$ can be derived using three image data embedding rules, respectively. We may obtain these $p_{v'}(v'|w)$ as follows

(By rule 1) $$p_{v'}(v'|w) = p_x(v'_i - \alpha w_i) = \frac{\beta c}{2\Gamma(1/c)} exp\{-\beta|v'_i - \alpha w_i|^c\} \qquad (1)$$

(By rule 2) $$p_{v'}(v'|w) = \frac{1}{1+\alpha w_i} p_x\left(\frac{v'_i}{1+\alpha w_i}\right) = \frac{\beta c}{2\Gamma(1/c)(1+\alpha w_i)} exp\left\{-\beta\left|\frac{v'_i}{1+\alpha w_i}\right|^c\right\} \qquad (2)$$

(By rule 3) $$p_{v'}(v'|w) = \frac{1}{1-\alpha} p_x\left(\frac{v'_i - \alpha w_i}{1-\alpha}\right) = \frac{\beta c}{2(1-\alpha)\Gamma(1/c)} exp\left\{-\beta\left|\frac{v'_i - \alpha w_i}{1-\alpha}\right|^c\right\} \qquad (3)$$

According to the approach proposed in [16], to derive the channel capacity for each use of the channel, i.e. the capacity of each coefficient, both the input w and the output v' of the channel are quantized, thus leading to a discrete input and discrete output model. By assuming DCT coefficients are independent each other, and by noting that w_i are i.i.d. random variables, we know that the watermark channel is a memoryless one.

After the input w and the output v' of the watermark channel are quantized respectively, the channel can be completely described by the discrete input set $\{\hat{w}_1, \hat{w}_2, \Lambda, \hat{w}_K\}$, the discrete output set $\{\hat{v}_1, \hat{v}_2, \Lambda, \hat{v}_J\}$ and the channel transition matrix $P = \{p(\hat{v}'_j | \hat{w}_k)\}_{K \times J}$, where $\hat{w}_i$ and $\hat{v}'_i$ indicate the *i*-th input and output quantized values respectively. $p(\hat{v}'_j | \hat{w}_k)$ can be calculated by integrating the conditional pdf in equation (1), (2), and (3), respectively. We should get

$$p(\hat{v}'_j | \hat{w}_k) = \int_{\hat{v}_j}^{\hat{v}_{j+1}} p_{V'}(v' | \hat{w}_k) dv' = \frac{\beta c}{2\Gamma(1/c)} \int_{\hat{v}_j}^{\hat{v}_{j+1}} exp\{-\beta | v' - \alpha \hat{w}_k |^c\} dv' \tag{4}$$

$$p(\hat{v}'_j | \hat{w}_k) = = \frac{\beta c}{2\Gamma(1/c)(1+\alpha w_k)} \int_{\hat{v}_j}^{\hat{v}_{j+1}} exp\{-\beta \left| \frac{v'}{1+\alpha w_k} \right|^c\} dv' \tag{5}$$

$$p(\hat{v}'_j | \hat{w}_k) = \frac{\beta c}{2(1-\alpha)\Gamma(1/c)} \int_{\hat{v}_j}^{\hat{v}_{j+1}} exp\{-\beta \left| \frac{v' - \alpha \hat{w}_k}{1-\alpha} \right|^c\} dv' \tag{6}$$

By [9], if we have obtained the channel transition matrix P, and the a-priori probabilities $p(\hat{w}_i)$, mutual information is defined as

$$I(W;V') = \sum_j \sum_k p(\hat{w}_k) p(\hat{v}_j | \hat{w}_k) log \frac{p(\hat{v}_j | \hat{w}_k)}{\sum_i p(\hat{w}_i) p(\hat{v}_j | \hat{w}_i)} \tag{7}$$

According to [9], the maximization of equation (7) over all possible sets of input probabilities gives the capacity of each DCT coefficient. Since the mutual information of a discrete memoryless channel is a convex function[9] of

$$p(W) = \{p(\hat{w}_1), p(\hat{w}_2), ..., p(\hat{w}_K)\},$$

the watermark channel capacity, then, can be obtained numerically by maximizing I(*W*; *V*') over the *K* variables $\{p(\hat{w}_k)\}$, subject to constraints:

$$p(\hat{w}_k) \geq 0, \quad \forall k$$

$$\sum_{k=1}^{K} p(\hat{w}_k) = 1$$

3 Decide Test Parameters

To estimate the channel capacity, some parameters have to be decided. Such as the quantization range of the output variable v', the strength factor α, and the input (output) quantization values have to be estimated.

3.1 Estimation the Quantization Range of the Output Variable v'

From the theoretical point of view, probability density function of camouflage image coefficients can be define at the whole real axle, so its quantization range can be assume is infinite. However, if we neglect the quantization range that probability is smaller than 10^{-4} in calculating actually, and notice probability density function of v' about ordinate axis symmetry, we should obtain quantization range of the output variable v' through the following relation holds

$$\int_{\hat{v}_J}^{+\infty} p_{V'}(v') dv' = \frac{\beta c}{2\Gamma(1/c)} \int_{\hat{v}_J}^{+\infty} exp\{-\beta | v' |^c\} dv' \leq \frac{1}{2} \times 10^{-4} \tag{8}$$

After deciding $\hat{v}_J$, notice $\hat{v}_1 = -\hat{v}_J$, the quantization range $[\hat{v}_1, \hat{v}_J]$ of variable *v*' can be obtained finally.

3.2 Estimation the Input (Output) Quantization Values

According to square error minimum we may fix the quantizing value, i.e., make

$$\varepsilon = E\{(x-y)^2\} = \int_{\hat{v}_1}^{\hat{v}_J} (x-y)^2 p_x(x)dx = \sum_{k=1}^{J} \int_{d_k}^{d_{k+1}} (x-y)^2 p_x(x)dx \quad (9)$$

receive the minimum, deriving process in [18]. The algorithm is described as follows

1) To choose $y_1 \in (\hat{v}_1, \hat{v}_J)$, arbitrarily;
2) Calculate out $\hat{v}_2$ using $\int_{\hat{v}_1}^{\hat{v}_2} (x-y_1)^2 p_x(x)dx = 0$;
3) Calculate out $y_2 = 2\hat{v}_2 - y_1$;
4) Continue this process until calculating out y_{J-1};
5) Within the range of given error (Error range in this paper is $<10^{-4}$), we will text whether or not y_{J-1} is the probability centre from $\hat{v}_{J-1}$ to $\hat{v}_J$, i.e.

$$\int_{\hat{v}_{J-1}}^{\hat{v}_J} (x-y_{J-1})^2 p_x(x)dx = 0 \quad (10)$$

If equation (10) is satisfied, the algorithm finishes. Otherwise, choose another y_1 and repeat this algorithm.

4 Experiments and Results

In order to analyses and compare the performance of three kinds of image data embedding rules, image data embedding process is considered to be a watermark channel, we should estimate their channel capacity respectively.

In the experiment, we compute DCT of each selected original image and secret image respectively at first, $\{v_i\}$ and $\{w_i\}$ indicate their DCT coefficients respectively. Standard deviation of $\{v_i\}$ is calculated out. The quantization range of $\{v_i\}$ is decided by equation (8). $\{v_i\}$ and $\{w_i\}$ are quantized respectively. According to equations (4), (5) and (6), the channel transition matrix corresponding with three kinds of image data embedding rules can be calculated out, respectively. Utilize (7) we can evaluate their channel capacities.

In order to observe the original image standard deviation influence to the watermark channel capacity, we choose different image carry on experiment, experimental results can be seen table 1 or figure 2.

Table 1. *The original image standard deviation influence to the watermark channel capacity (Bit), where* α =0.034, *c*=1

σ rule	0.2588	0.5076	0.7564	1.0052	1.2540	1.5028	1.7516	2.0000
1	0.0063	0.0024	0.0015	0.0012	0.0011	0.0010	0.000961	0.000933
2	0.0010	0.0010	0.0010	0.0010	0.0010	0.0010	0.0010	0.0010
3	0.0067	0.0025	0.0016	0.0013	0.0011	0.0010	0.000976	0.000941

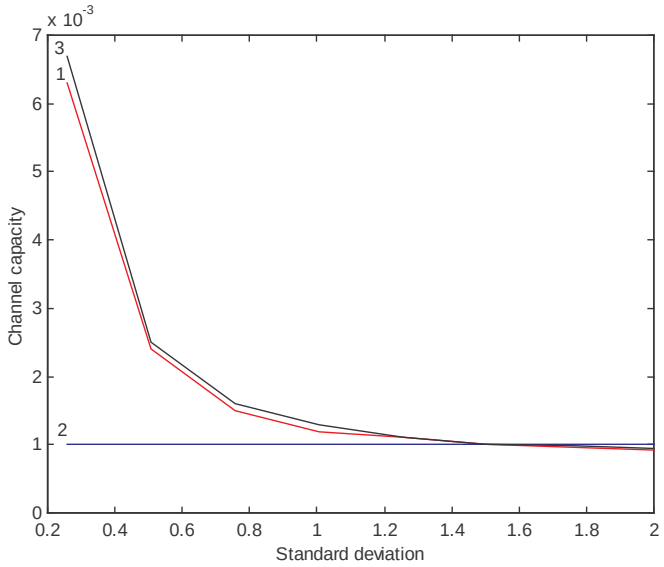

Figure 2.
The original image standard deviation Influence to the watermark channel capacity (Bit), where α =0.034 *and c*=1

By observation table 1 or figure 2, we can find the second kind of image data embedding rule is free for standard deviation change, 0.001Bit average can be hid in each DCT coefficient using this embedding rule. Another two kinds of image data embedding rules are affected greatly by standard deviation change, with the increase of the coefficient standard deviation, the watermark channel capacity drops rapidly. In fact, as the coefficient standard deviation is very small, data of original image tend towards zero, there is not an actual meaning at this situation. When the standard deviation is greater, watermark channel capacity approach zero, this proves that the original image can't be used for hiding the secret image in this case.

In this example, when α =0.034, c=1 and 0.3< σ <1.2, the first and third kinds of image data embedding rules average can hide more Bit information than second kind of image data embedding rule in each DCT coefficient. That is to say, when 0.3< σ <1.2, from the view point of hiding the amount of information, the first and third kinds of embedding rules can hide more information than the second kind of embedding rule within same original image.

In order to observe the strength factor α and shape parameter c of the generalized Gaussian distribute effect on watermark channel capacity, we let c=0.6, c=1 and c=10 respectively, and let the strength factor α be different value, we estimate watermark channel capacity using three image data embedding rules, respectively. Our estimation results are in table 2, table 3 and table 4, or figure 3 and figure 4.

Table 2. *Effect of varying strength factor* α *on watermark channel capacity, where c*=0.6

α rule	0.024	0.034	0.044	0.054	0.064	0.074	0.084	0.094
1	0.000011	0.000049	0.000123	0.000241	0.000331	0.000407	0.000476	0.000542
2	0.000706	0.000720	0.000754	0.000791	0.000828	0.000871	0.000913	0.00096
3	0.00410	0.00740	0.0106	0.0153	0.0200	0.0258	0.0315	0.0377

Table 3. *Effect of varying strength factor* α *on watermark channel capacity, where c*=1

α rule	0.024	0.034	0.044	0.054	0.064	0.074	0.084	0.094
1	0.0016	0.0022	0.0029	0.0041	0.0056	0.0072	0.0091	0.0117
2	0.0013	0.0014	0.0015	0.0017	0.0019	0.0021	0.0024	0.0028
3	0.0020	0.0028	0.0039	0.0053	0.0067	0.0091	0.0115	0.0142

Table 4. *Effect of varying strength factor* α *on watermark channel capacity, where c*=10

rule \ α	0.024	0.034	0.044	0.054	0.064	0.074	0.084	0.094
1	0.0017	0.0028	0.0037	0.0049	0.0063	0.0079	0.0097	0.0117
2	0.0016	0.0026	0.0034	0.0048	0.0061	0.0078	0.0095	0.0115
3	0.0019	0.0032	0.0045	0.0067	0.0088	0.0118	0.0147	0.0183

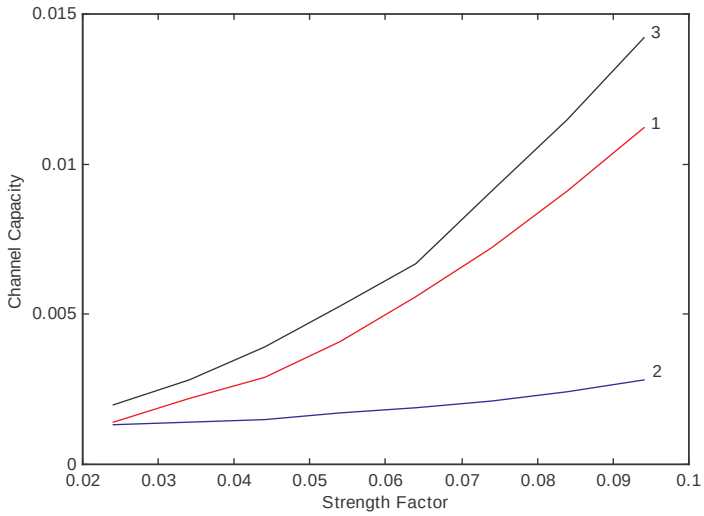

Figure 3. *Effect of varying strength factor* α *on watermark channel capacity, where c*=1

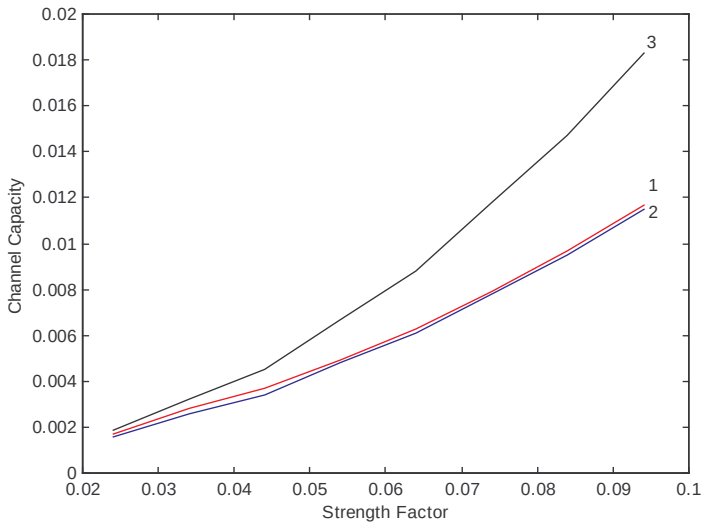

Figure 4. *Effect of varying strength factor* α *on watermark channel capacity, where c*=10

To utilize the first and the second kind of image data embedding rules for DCT coefficients of the same original image, by observation and analysis to table 2, we may find that the secret information average can be hidden in each DCT coefficient is very little, when c=0.6. That is to say, if c is very small, the first and the second kind of image data embedding rules aren't suitable to hide secret image. By contrast, the third kind of embedding rule average can hide more information to each DCT coefficient. So, when c<1, we should adopt the third kind of embedding rule for hiding secret image.

When c≥1, by observation table 3 and table 4, we may find that the secret information to be hidden in each DCT coefficient average is the most using the third kind of embedding rule, the secret information is the least using the second the embedding rule, and the secret information is between the first and the second kind of embedding rules using the first embedding rule. This indicates that the three kinds of embedding rules can all be used for hiding the secret image. At using actually, we should adopt the suitable embedding rule according to the practical problem.

By observation table 2, 3 and 4, we may find that the watermark channel capacity increase fast with increase of c when using first and the second embedding rules, but not like this to the third kind of embedding rule. When using the third kind of embedding rule, channel capacity of $c < 1$ far exceed channel capacity of $c \geq 1$, even c is very small, so is it, too. These performances have offered basis on which we use the three kinds of embedding rules better.

When the strength factor α increases, no matter $c<1$ or $c \geq 1$, the watermark channel capacity increases too. However, a higher capacity results in the former case, this does not mean that by embedding the secret image in the DCT domain a higher capacity can be achieved, since to ultimately decide which embedding rule ensures a higher capacity, the visibility of the secret image should be taken into account as well.

5 Conclusion and Future Work

Utilize the information theory, we analyze and compare about the performance of three kinds of image data embedding rules. If simple from the point of view of channel capacity, because the watermark channel capacity of the third kind of embedding rule is always higher than another two kinds of embedding rule's, so it equally can hide more Bit information in each DCT coefficient within the same image according to the third embedding rule by means of frequency domain. Therefore, this kind of embedding rule is more suitable for hiding the secret image. Because hidden information in each DCT coefficient don't rely on change of standard deviation of original image, if standard deviation of original image is unstable (or not know), second embedding rule is suitable for hiding secret image.

Future research will focus on the extension of the above analysis to the evaluation of the impact that the constraints on secret image invisibility. Besides, proper channel models have to be developed to take into account attacks, since attacks appear to be the most important limitation to the reliable concealment and retrieval of information within digital images.

References

1. M.D.Swanson, M.Kolayashi, and A.H.Tewfik. (1998) Multimedia Data Embedding and Watermarking Technologies. Proc. of IEEE, 86, 6, 1064-1087
2. F.Hartung and M.Kutter. (1999) Multimedia Watermarking Techniques. Proc. of The IEEE, 87,7, 1079-1107
3. G.J.Simmons. (1984) The Prisoner's Problem and the Subliminal Channel. Advances in Cryptography. Proceedings of CRYPTO'83, 51-67
4. S.Kstzenbeisser and F.A.Petitcolas. (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Artech House/ Boston
5. C.C.Chang, T.S.Chen, and C.S.Tsai, (2000) A New Scheme for Sharing Secret Color Images in Computer Network. Proceedings of International Conference on Parallel and Distributed Systems, 21-27
6. B.Pfitzmann, (1996) Information Hiding Terminology. In Lecture Notes in Computer Science, 1174(1996), Berlin, Germany/Springer-Verlag
7. J. R. Hernandez and F. Perez-Gonzalez. (1999) Statistical Analysis of Watermarking Schemes for Copyright Protection of Images. Proceedings of the IEEE, 87, 1142-1166
8. I.J.Cox., J.Killian, F.Thomson, and T.Shamoon. (1997) Secure Spread Spectrum Watermarking for Multimedia. IEEE Transaction on Image Processing, 6, 1673-1687
9. R.G. Gallager. (1968) Information Theory and Reliable Communication. Wiley/ New York
10. B.Chen, G.W.Wornell. (1999) An Information-Theoretic Approach to the Design of Robust Digital Watermarking Systems. Proc. Int. Conf. on Acoustics, Speed and Signal Processing (ICASSP), Phoenix, AZ
11. P.Moulin. (2001) The Role of Information Theory in Watermarking and Its Application to Image Watermarking. Signal Processing, 81,6, 1121-1139
12. F.M.J. Willems. (2000) An Information Theoretical Approach to Information Embedding. Proc. 21st Symp. Info. Thy in the Benelux, Wassenaar/The Netherlands, 255-260
13. J.R.Smith and B.O.Comiskey. (1996) Modulation and Information Hiding in Images. In Proc. of First Int. Workshop on Information Hiding, Lecture Notes in Computer Science, 1174, 207-226
14. S.D.Servetto, C.I.Podilchuk, and K. Ramchandran. (1998) Capacity Issues in Digital Image Watermarking. In Proc. ICIP'98, IEEE Int. Conf. on Image Processing, I (Chicago, Illinois, USA) , 445-449
15. T.Kalker, J.P.Linnartz, G.Depovere, and M.Maes, (1998) On the Reliability of Detecting Electronic Watermarks in Digital Images. In Proceedings of EUSIPCO'98, Ninth European Signal Processing Conference, Rodos/ Greece, 13-16
16. M.Barni, F.Bartolini, A. De Rosa, and A. Piva. (1999) Capacity of the Watermark-Channel: How Many Bits Can Be Hidden Within a Digital Image? In Security and Watermarking of Multimedia Contents, Wong, Delp, Editors, Proceedings of SPIE 3657, San Jose, CA ,437-448
17. R.J.Clarke, (1985) Transform Coding of Images, Academic Press
18. J. Max. (1960) Quantization for Minimum Distortion , IRE Trans., IT-6, 2, 7-12

Article received: 2005-06-23