Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **4**, July **2016**

Information Hiding Capacities in Different Multiple Antenna Systems

Li-Quan Chen, Zi-Juan Fan, Miao Lu, Ai-Qun Hu

School of Information Science and Engineering
Southeast University
Nanjing, China, 210096
lqchen@seu.edu.cn, zjfan@seu.edu.cn, lm871006@126.com, aqhu@seu.edu.cn

Received Februrary, 2015; revised August, 2015

Abstract. *The information hiding processing based on channel coding in multiple antenna systems is analyzed. Based on the theory of information hiding capacity in single coding channel, the effect of transmit diversity, receive diversity, space-time coding and MIMO technologies on hiding capacity in multiple antenna systems is presented and analyzed. Simulation results show that these technologies can improve the reliability of information hiding algorithms in multiple antenna systems, and reduce the effect of channel interference on transmitted data by antenna diversity and space-time coding schemes. The hiding capacity performance is improved based on these multiple antenna technologies. When SNR is 10dB, the hiding capacity ratios with 2Tx diversity,* 2×2 *MIMO and* 2×1 *STC are higher than that of an information hiding system with 1Tx×1Rx. If SNR becomes 20dB, the hiding capacity ratios are enhanced too, but the enhancement is smaller.*

Keywords: Multiple antenna system; Information hiding; MIMO; Hiding capacity; Transmit diversity; Receive diversity.

1. **Introduction.** Traditional information carriers such as text, image, audio, video and other digital medias are generally used in information hiding, but the information hiding systems based on these carriers will change the statistical properties of the original carriers, thus lead to the suspicion of attackers [1]. The information hiding technology based on channel coding carrier is a new information hiding research field[2] [3] [4] [5]. When the secret data is embedded into the channel coding data carrier as part of noise, and if the total errors caused by secret data and channel interference are no more than the errors correcting capability of the coding channel, both the normal communication and the information hiding function can be achieved.

In multiple antenna system, multiple antennas are used in both the transmitter and receiver. The transmission signals are processed by space-time coding techniques, and the communication link is divided effectively into several parallel sub-channels to transmit data [6] [7]. The advantage of multiple antenna technology is that the data rate and quality of wireless communication can be improved without increasing the transmitting power and channel bandwidth.

Capacity of information hiding system is an important performance index for an information hiding system [8] [9] [10]. A good information hiding system should not only meet the demands of imperceptibility, robustness and security, but also reach the information hiding capacity's upper bound as much as possible. Information hiding system based on channel coding requires that the total errors caused by the secret data replacement and channel interference do not exceed the error correcting capability of the coding channel. Therefore, under the same conditions, if the errors caused by channel interference can be minimized, we can embed more secret data, and the information hiding capacity can be improved. For multiple antenna system, the bit error rate (BER) performance of the channel can be effectively improved by space-time processing. In consequence, the analysis of information hiding capacity in multiple antenna systems is of great significance.

The rest of the paper is organized as follows. In section 2, the information hiding capacity in multiple antenna systems is presented and analyzed. In section 3, the effects of multiple antenna technologies on information hiding capacities are analyzed and the capacity equations are presented. Next, simulation and analysis are done in section 4. Finally, conclusion is given in section 5.

2. Information hiding capacity in multiple antenna systems.

2.1. Information hiding in multiple antenna systems. We consider a multiple antenna channel with n_T transmitting antennas and n_R receiving antennas, then a $n_R \times n_T$ complex channel matrix H is constructed. The vector $h_{j,i}$ is referred to as the channel's fading coefficients from the ith ($i = 1, 2, \cdots, n_T$) transmit antenna to the jth ($j = 1, 2, \cdots, n_R$) receive antenna. Then

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n_T} \\ h_{21} & h_{22} & \cdots & h_{2n_T} \\ \vdots & \vdots & \vdots & \vdots \\ h_{n_R1} & h_{n_R2} & \cdots & h_{n_Rn_T} \end{bmatrix}_{n_R \times n_T}, \tag{1}$$

the multiple antennas' mathematical model can be expressed as

$$y = Hx + n, \tag{2}$$

where $x = (x_1, x_2, \cdots, x_{n_T})^T$ is the $n_T \times 1$ transmitted signal vector, x_i represents the signal transmitted by the ith antenna. $y = (y_1, y_2, \cdots, y_{n_R})^T$ is the $n_R \times 1$ received signal vector, y_j is the signal received by the jth antenna, $n = (n_1, n_2, \cdots, n_{n_R})^T$ is the $n_R \times 1$ complex Gaussian noise vector, n_j represents the noise received by the jth antenna. All the elements of noise vector n and matrix H are independent and identically distributed as complex Gaussian random variables with zero mean. And X^T represents the transposed matrix of X, X^H represents the conjugated matrix of X, $E(\bullet)$ means the mathematical expectation.

The structure of information hiding system based on channel coding in multiple antenna system is shown in Figure 1. Here, multiple antenna processing module is added to an information hiding system, the secret data is embedded in the channel coding bit stream, which is encoded by space-time coding techniques and transmitted by multiple antennas. At the receiver side, the secret data is extracted by information extracting techniques, and the carrier bit stream data is decoded. Here, error correcting code (ECC) is used before secret data is embedded after extraction. It can help to improve the hiding performance of the whole system.

In Figure 1, the bit embedding algorithm can be the normal spatial domain or transform domain information hiding algorithm. Here, since we want to find out the effect of multiple antenna system on information hiding, the least significant bit (LSB) replacement information hiding algorithm is used, and no preprocessing method is used before the LSB embedding. In the LSB replacement algorithm, we use the secret bits to replace all the

LSB bits in the carrier data so as to analyze and test the information hiding capacities in multiple antenna systems.

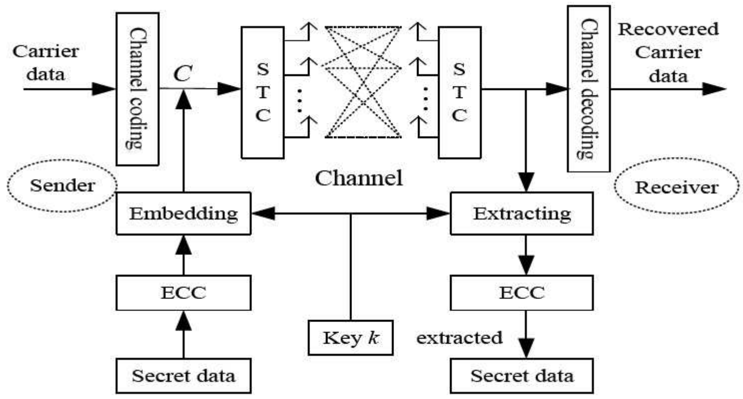


Figure 1. Information hiding based on channel coding in multiple antenna system

2.2. **Information hiding capacity based on channel coding.** Taking the error correcting capability of the coding channel into consideration, before information hiding, it must be ensured that the total errors caused by secret data replacement and channel interference doesn't exceed the capability, only by then can the carrier source data be received without error and the secret data be extracted accurately at the receiver side.

The bases of information hiding capacity in coding channel is that the bit size of secret data replacement plus the errors of carrier data caused by channel interference, minus the errors of secret data caused by channel interference should be less than the error correcting capability of the coding channel [11]. So the information hiding capacity in coding channel system is the largest number of embedded bits based on the above constrain. In multiple antenna systems, the information hiding capacity is defined similarly.

Here we present a channel block coding example to illustrate the theory analysis of information hiding capacity in coding channel.

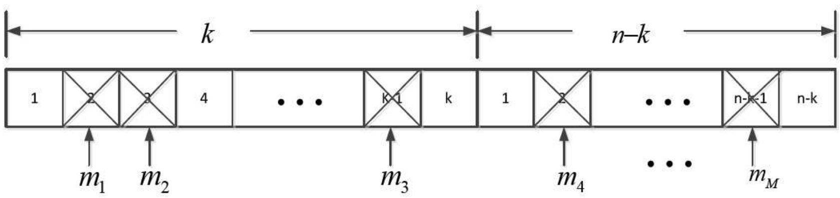


Figure 2. Example of information hiding in coding channel

Assuming that the channel coding parameters are (n, k, t), the bit error rate caused by channel interference is p_b. In Figure 2, $(m_1, m_2, \cdots, m_M)$ represent the secret data, k is the length of encoded input, n is the length of encoded output, t represents the number of error corrections in a single channel block coding. The secret data is embedded into the relevant position in channel coding block by replacing the original bit according to the LSB algorithm. In the worst case, when all the secret bits are contrary to the carrier source bits at the hiding positions, that is, for the source data stream, the secret data completely becomes interference. They are represented by $\times$ in Figure 2. So the most errors caused by secret data are M bits. However, the secret bits embedded in the carrier data stream also become error bits when the carrier is transmitted through the channel.

Therefore, the errors caused by secret information cannot be double counted. Then the errors caused by channel interference are calculated as $(n - M) \cdot p_b$. In summary, if $M + (n - M) \cdot p_b \le t$, the total errors caused by secret data and channel interference can be represented as $M + (n - M) \cdot p_b$.

The capacity of information hiding system based on channel coding is analyzed as follows. Here we assume that C_0 is the length of carrier source data, C is the length of source data after channel encoding, $m_0 = (m_{01}, m_{02}, \cdots, m_{0M_0})$ is the secret data stream, $m = (m_1, m_2, \cdots, m_M)$ is secret data after preprocessing. $E(C, m, K)$ is the embedding algorithm for secret data and $D(C', K)$ is the extracting algorithm for secret data. M_0 is the length of secret data, M is the length of secret data after preprocessing, K is the secret key shared by both side and is used to generate pseudo-random sequence to determine the positions for secret data embedding. P_b is the bit-error-rate of the channel.

Assuming that the channel coding method is block coding and the parameters are (n_1, k_1, t_1) . In an ideal case of error correcting, the capacity of information hiding system based on channel coding is

$$M + (C \cdot P_b - M \cdot P_b) \le \frac{C}{n_1} \cdot t_1, \tag{3}$$

then, we get

$$M \le \frac{\frac{C}{n_1} \cdot t_1 - C \cdot P_b}{1 - P_b}, \tag{4}$$

finally,

$$M_{\max} = \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot P_b}{1 - P_b}. \tag{5}$$

If the size of the secret data remains unchanged after preprocessing, the capacity of information hiding system based on channel coding is $M_{\max}$. If the secret data is preprocessed by error correction coding method and the parameters are (n_2, k_2, t_2), the capacity of information hiding system based on channel coding becomes

$$M_{0\max} = \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot P_b}{1 - P_b} \cdot \frac{k_2}{n_2}. \tag{6}$$

3. Analysis of multiple antenna technologies on information hiding capacities.

3.1. Transmit diversity technique on information hiding capacity.

In transmit diversity technique, multiple antennas are used in transmitter while only one antenna is used in receiver. Assuming that the channel is a flat fading channel with N_T antennas in transmitter, then, in the same time-slot, the transmitted signal of each antenna is $x_i = \sqrt{\frac{P_T}{N_T}} w_i s, i = 1, 2, \cdots, N_T$, where s is the unit signal, w_i is the weight of transmitted signal, and $\|\vec{w}\|^2 = N_T$. The total transmitting power is P_T. $\vec{h} = [h_1, h_2, \cdots, h_{N_T}]$ represents the sub-channels of N_T transmitted signals, $\vec{n} = [n_1, n_2, \cdots, n_{N_T}]$ is the noise vector. Both h_i and n_i are the independent and symmetric complex Gaussian random variables with zero mean, and $\varepsilon\left(\vec{n}\vec{n}^H\right) = N_0 I_{N_T}$. Assuming that received signal is y, the transmitter diversity system can be expressed as

$$\vec{y} = \sqrt{\frac{P_T}{N_T}} \vec{h} \cdot \vec{w} \cdot s + \vec{n}. \tag{7}$$

If the signals are transmitted with equal power in the system, the received signal is then given by

$$\vec{y} = \sqrt{\frac{P_T}{N_T}} \sum_{i=1}^{N_T} h_i \cdot s + \vec{n}. \tag{8}$$

Because $\sum\limits_{i=1}^{N_T} h_i/\sqrt{N_T}$ is the independent and symmetric complex Gaussian random variable with zero mean, equation (8) can be simplified as

$$y = \sqrt{P_T} hs + n. \tag{9}$$

According to [12], if the channel knowledge is available in the transmitter, in order to maximize SNR, the weight vector of transmitted signal is needed to be

$$\vec{w} = \sqrt{N_T} \frac{\vec{h}^H}{\sqrt{\left\|\vec{h}\right\|^2}}. \tag{10}$$

Then, equation (9) can be transformed into

$$\vec{y} = \sqrt{\left\|\vec{h}\right\|^2 P_T} \cdot \vec{s} + \vec{n}, \tag{11}$$

the output SNR after transmitting through the channel is

$$SNR_{out} = \frac{\left\|\vec{h}\right\|^2 P_T}{N_0}. \tag{12}$$

According to [13] and [14] and Chernoff inequality $Q(x) \leq e^{-x^2}$, when the received SNR reaches maximum, the channel code element error rate of the diversity system is

$$P_e \leq N_e \prod_{i=1}^{N_T} \frac{1}{1 + \frac{P_T d_{min}^2}{4N_0}}, \tag{13}$$

where d_{min} represents the minimum Euclidean distance of the adjacent constellation points of the transmitted signal, N_e denotes the average number of signal points which includes d_{min}.

According to equation (13), when the received signal to noise ratio (SNR) reaches maximum, the upper limit BER of diversity system can be estimated. Moreover, the maximum information hiding capacity of transmit diversity system can be calculated based on equation (5). When M-ary modulation is used in the system, $M = 2^k$, and both bit error rate and code element error rate are uniformly distributed. That is to say, if and only if all the k bits are correct, code element can be received correctly. The relation between code element error rate and bit error rate is expressed as

$$p_b = 1 - (1 - p_e)^{\frac{1}{k}}. \tag{14}$$

According to equations (5),(13),(14), when the transmit diversity system reaches maximum SNR, the maximum information hiding capacity based on channel coding is

$$M_{\max} = \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot \left(1 - \left(1 - N_e \prod\limits_{i=1}^{N_T} \frac{1}{1 + \frac{P_T d^2{}_{\min}}{4N_0}} \right)^{\frac{1}{k}} \right)}{1 - \left(1 - \left(1 - N_e \prod\limits_{i=1}^{N_T} \frac{1}{1 + \frac{P_T d^2{}_{\min}}{4N_0}} \right)^{\frac{1}{k}} \right)} \cdot \frac{k_2}{n_2} \ . \tag{15}$$

In equation (15), channel coding parameters are (n_1, k_1, t_1), error correcting encode is used to pre-process the secret information and its parameters are (n_2, k_2, t_2), P_T is the total transmitting power, N_0 is the noise power and k is the number of bits contained in each code element.

Based on equation (15), the capacity of information hiding system can be estimated before the secret data is embedded. Taking the estimated capacity into account for information hiding, not only the utilization of information hiding system can be enhanced, but also the imperceptibility of the system can be ensured.

3.2. **Receive diversity technique on information hiding capacity.** In receive diversity system, multiple antennas are used in receiver while only one antenna is used in transmitter. Suppose that there are N_R antennas in receiver, then the transmitted signal can be expressed as $x = \sqrt{P_T} s$. Here, s is the signal unit, and $E\left(|s|^2\right) = 1$. $\vec{h} = [h_1, h_2, \cdots, h_{N_R}]$ represents the channel response of N_R received signals, $\vec{n} = [n_1, n_2, \cdots, n_{N_R}]$ represents the noise vector, and $\vec{y} = [y_1, y_2, \cdots, y_{N_R}]$ is the received signal vector. Then the receiver diversity system can be written as

$$\vec{y} = \sqrt{P_T}\vec{h}s + \vec{n}. \tag{16}$$

Suppose that the channel knowledge is available to receiver, the acceptance judgment is based on maximal ratio combining (MRC), the output data of receiver is

$$z = \sqrt{P_T}\vec{h}^H\vec{h}s + \vec{h}^H\vec{n} = \sqrt{P_T}\left\|\vec{h}\right\|^2 s + \vec{h}^H\vec{n}. \tag{17}$$

Comparing equation (17) with equation (11), when MRC is used to receive signal, the signal-to-noise ratio is the same as that in maximum ratio transmission, which is shown in reference [13]. So, the single input multiple output (SIMO) system based on MRC and the multiple input single output (MISO) system with the maximal received signal-to-noise share the same bit error rate (BER).

3.3. **Multiple input multiple output (MIMO) scheme on information hiding capacity.** Suppose that $\vec{x} = [x_1, x_2, \cdots, x_{N_T}]^T$ is the transmitted signal vector, $\vec{y} = [y_1, y_2, \cdots, y_{N_R}]$ is the received signal vector, H is a $N_R \times N_T$ complex channel matrix. The vector $h_{j,i}$ is referred as the channel fading coefficients from the ith $(i = 1, 2, \cdots, n_T)$ transmitting antenna to the jth $(j = 1, 2, \cdots, n_R)$ receiving antenna, then the relation between transmitted signal and received signal is presented as

$$y_i = \sum_{j=1}^{N_T} h_{ij}x_j + n_i. \tag{18}$$

Assuming that the same signal is transmitted by transmitting antenna in the same time-slot, the transmitted signal is then given by

$$\vec{y} = \sqrt{\frac{P_T}{N_T}} H \cdot \vec{w} \cdot s + \vec{n}. \tag{19}$$

Processing the N_R received signals, we can get

$$z = \vec{p}^H\vec{y} = \sqrt{\frac{P_T}{N_T}}\vec{p}^H H\vec{w}s + \vec{p}^H\vec{n}, \tag{20}$$

where $\vec{p}$ is a $N_R \times 1$ vector. As the matrix H can be singular value decomposed to $H = U\Lambda V^H$, while U is a $N_R \times N_R$ unitary matrix, V is a $N_T \times N_T$ unitary matrix, $\Lambda = diag\left\{\sigma_1, \sigma_2, \cdots \sigma_r\right\}$ is the singular value of channel matrix. As shown in [14], if $\vec{p}$ and $\vec{w}/\sqrt{N_T}$ correspond to the column vectors of U and V respectively, the result of $\vec{p}^H H \frac{\vec{w}}{\sqrt{N_T}}$

should then correspond to the maximal singular value $\sigma_{\max}$, which is the maximum of SNR. Therefore, if $\vec{p}$ and $\vec{w}$ is taken appropriately, equation (20) can be simplified into

$$z = \sqrt{P_T}\sigma_{\max} s + n. \tag{21}$$

For channel parameters H and $\sigma_{\max}$, they should meet

$$\frac{\|H\|^2}{r} \le {\sigma_{\max}}^2 \le \|H\|^2. \tag{22}$$

Therefore, the SNR of received signal in MIMO system is restricted as [15]

$$\frac{P_T \max(N_T, N_R)}{N_0} \le SNR \le \frac{P_T N_T N_R}{N_0}. \tag{23}$$

According to [16], we get that

$$N_e \prod_{i=1}^{N_T N_R} \frac{1}{1+\frac{P_T {d^2}_{\min}}{4N_0}} \le p_e \le N_e \prod_{i=1}^{N_T N_R} \frac{1}{1+\frac{P_T {d^2}_{\min}}{4N_0 \min(N_T, N_R)}} \ . \tag{24}$$

As indicated in equation (24), compared with the single-antenna system, the MIMO technology can make the bit error rate decrease exponentially with $N_T N_R$. According to equations (6),(15) and (24), the upper limit of information hiding capacity in BPSK-MIMO system based on channel coding is given by

$$M \le \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot \left(1 - \left(1 - N_e \prod_{i=1}^{N_T N_R} \frac{1}{1+\frac{P_T {d^2}_{\min}}{4N_0}} \right)^{\frac{1}{k}} \right)}{1 - \left(1 - \left(1 - N_e \prod_{i=1}^{N_T N_R} \frac{1}{1+\frac{P_T {d^2}_{\min}}{4N_0}} \right)^{\frac{1}{k}} \right)} \cdot \frac{k_2}{n_2} \ . \tag{25}$$

3.4. **Space-time coding techniques on information hiding capacity.** Space-time coding techniques can improve the reliability of a communication system, thus can increase the information hiding capacity of this system. When a channel coding method is selected, the reduction of the errors caused by channel interference is equivalent to the increase of the information hiding capacity.

Take the 2×1 Alamouti system into consideration, we analyze the effect of space-time coding technique on information hiding capacity. Suppose binary phase shift keying (BPSK) modulation is used in the MIMO information hiding system, the channel between two transmitting antennas and one receiving antenna is quasi-static channel, the channel fading coefficients remain unchanged in one frame time, and the fading coefficients are independent and identically distributed as complex Gaussian random variables. The signals are transmitted with equal power in the system and the channel parameters are known to the receiver.

Suppose that $\{x_1, x_2\}$ is a pair of transmitted signal, $\{r_1, r_2\}$ are the received signals in one time slot, the relations between them are

$$r_1 = h_1 x_1 + h_2 x_2 + n_1 \text{ and} \tag{26}$$

$$r_2 = -h_1 {x_2}^* + h_2 {x_1}^* + n_2. \tag{27}$$

When MRC is used in receiver, the received signals are then constructed as

$$\begin{aligned}\tilde{x}_1 &= {h_1}^* \cdot r_1 + h_2 \cdot {r_2}^* \\ &= \left(|h_1|^2 + |h_2|^2\right) \cdot x_1 + {h_1}^* \cdot n_1 + h_2 \cdot {n_2}^*,\end{aligned} \tag{28}$$

$$\begin{aligned}\tilde{x}_2 &= {h_2}^* \cdot r_1 - h_1 \cdot {r_2}^* \\ &= \left(|h_1|^2 + |h_2|^2\right) \cdot x_1 + {h_2}^* \cdot n_1 - h_1 \cdot {n_2}^*.\end{aligned} \tag{29}$$

Take x_1 for example, the received signal power and noise power are

$$S_{\tilde{x}_1} = \left(|h_1|^2 + |h_2|^2\right)^2 \cdot \frac{P_T}{2}, \tag{30}$$

$$N_{\tilde{x}_1} = \left(|h_1|^2 + |h_2|^2\right) \cdot N_0. \tag{31}$$

Therefore, the SNR of receiver is:

$$\gamma_o = \frac{S_{\tilde{x}_1}}{N_{\tilde{x}_1}} = \left(|h_1|^2 + |h_2|^2\right) \cdot \frac{P_T}{2N_0} = \frac{\left(|h_1|^2+|h_2|^2\right)}{2} \cdot \gamma_s \ . \tag{32}$$

According to equation (32), the SNR in receiver is proportional to the SNR in transmitter if the channel is determined. Thus, for the sake of simplicity we analyze the SNR in transmitter instead of SNR in receiver.

According to [13], the BER of BPSK transmission signal is equivalent to

$$P_b = Q\left(\sqrt{\left(|h_1|^2 + |h_2|^2\right) \cdot \gamma_s}\right), \tag{33}$$

where $Q(x) = \frac{1}{2} \cdot erfc\left(\frac{x}{\sqrt{2}}\right)$, $\gamma_s = \frac{P_T}{N_0}$. According to [17], when the above distributions are met, the average bit-error probability is calculated as

$$p_b = \frac{1}{4}\left(1 - \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)^2 \left(2 + \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right) . \tag{34}$$

Based on the equation (6),(15) and (34), the information hiding capacity in Alamouti space-time coding system based on channel coding is

$$M = \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot \frac{1}{4}\left(1 - \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)^2 \left(2 + \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)}{1 - \frac{1}{4}\left(1 - \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)^2 \left(2 + \frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)} \cdot \frac{k_2}{n_2}. \tag{35}$$

4. **Simulation and analysis.** Before doing simulation and analysis, we define the hiding capacity ratio which can exactly reflect the information hiding capacity in multiple antenna systems.

$$\text{hiding capacity ratio} = \frac{\text{the length of secret data}}{\text{the length of encoded source data}}$$

Now we can perform numerical analysis on the hiding capacity ratio of each multiple antenna system. For example, according to the equation (35), the information hiding capacity of the Alamouti space-time coding channel is ascertained as long as the SNR value is increasing while the channel coding method are fixed. Assuming that 128×256

Table 1. SNR values vs. the theoretical values of hiding capacity ratios

SNR/dB	No Diversity 1Tx, 1Rx	Tx Diversity 2Tx, 1Rx	Rx Diversity 1Tx, 2Rx
10	0.0562	0.0656	0.0656
20	0.0841	0.0851	0.0851
SNR/dB	MIMO 2Tx, 2Rx	STC Alamouti 2Tx, 1Rx	
10	0.0884	0.0609	
20	0.0923	0.0846	

low density parity check (LDPC) code is used in channel coding, the length of source data is 10000 bits, the length of source data after channel encoding is 20224 bits and the SNR is 20dB. The information hiding capacity is then presented as

$$M = \left\lceil \frac{C_0}{k_1} \right\rceil \frac{t_1 - n_1 \cdot \frac{1}{4}\left(1-\frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)^2\left(2+\frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)}{1-\frac{1}{4}\left(1-\frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)^2\left(2+\frac{1}{\sqrt{1+\frac{2}{P_T/N_0}}}\right)} \cdot \frac{k_2}{n_2} = 1710 bits \ .$$

Thus,

$$\text{hiding capacity ratio} = \frac{\text{the length of secret data}}{\text{the length of encoded data}} = \frac{1710}{20224} = 0.0846 \ .$$

In Table 1, we present the different hiding capacity ratio according to different SNR values in different multiple antenna transmission systems. We can find out that with the increasing of the antenna number, the information hiding capacity ratio is increased.

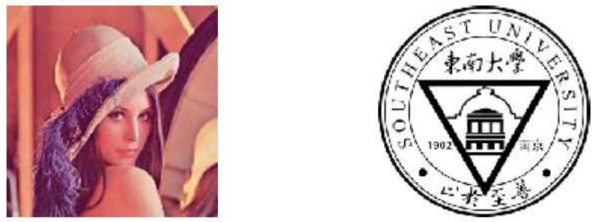
4.1. **BER performance analysis of information hiding capacity in multiple antenna systems.** The simulation parameters are set as follows. We take the color image lena.tiff with 768K Bytes in size as carrier data, and the secret data is an image of Southeast University logo in size of 19K Bytes.

Figure 3 shows the extracted carrier image and the extracted secret image when information hiding capacity exceeds the maximum error correcting capability of channel coding. Here, the simulation channel is additive white Gaussian noise (AWGN) channel and SNR is 10dB. From Figure 3 we can find out that if one information hiding algorithm exceeds the maximum error correcting capability of one MIMO system, the effects of extracted carrier image and secret image all become bad.

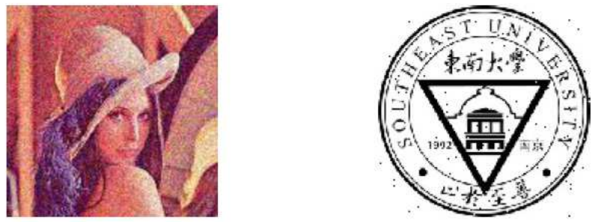
We have also done the simulation based on baboon.tiff, barbara.tiff and the other standard test pictures as the carrier data. The simulation results are the same as those based on lena.tiff.

Then we do the other simulations to get the different BER performances vs. different techniques and different SNR values. Suppose that the carrier is based on (63, 30, 6) bose, ray, hocquenghem (BCH) channel code, the secret image uses (15, 7, 4) reed solomon (RS) error correcting code, the modulation method is BPSK, the channel is a flat Rayleigh fading channel. If Alamouti space-time coding is used, then there are two transmitting antennas and one receiving antenna in the system and the signals are transmitted with the same power in the transmitter. Or else, there are one transmit antenna and two receive antennas in the system and MRC is used to receive signals at the receiver. The simulation results of information hiding algorithm based on channel coding in multiple antenna systems are shown in Figure 4 and Figure 5.

In Figure 4, the three curves represent different BER performances of source data when space-time processing is absent, when Alamouti space-time coding is used and when receiver diversity technique is used. According to Figure 4, the BER values of the source



(a) the original carrier image and the secret image



(b) the extracted carrier image and the extracted secret image

Figure 3. Information hiding results when hiding capacity is exceeded

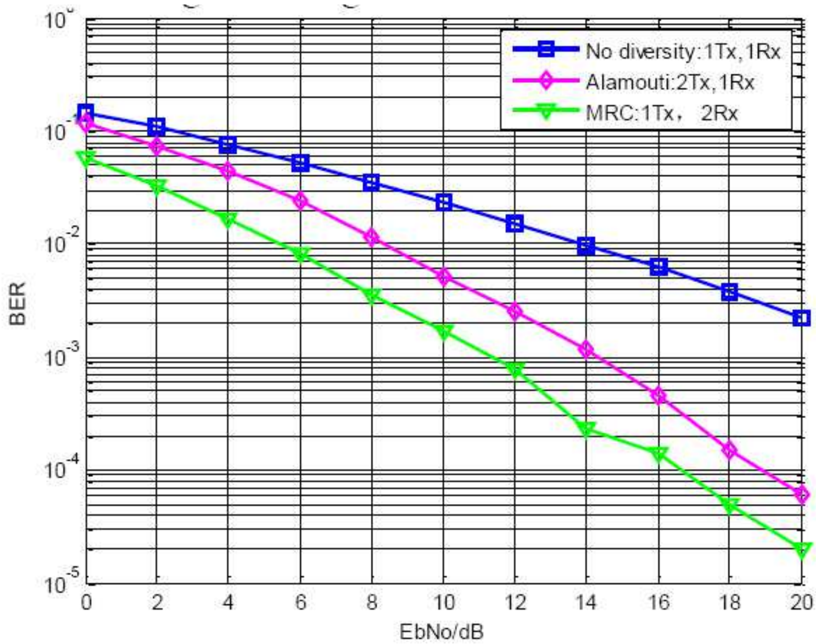


Figure 4. BER of source data vs. SNR in multiple antenna system simulation

data in 2Tx, 1Rx antennas transmission scheme and Alamouti space-time coding scheme are better than those in 1Tx, 1Rx transmission scheme when SNR is the same. The reason is that two types of code elements which satisfy orthogonal relation are transferred in two slots after space-coding, thus the receiver can get the transmitted signal more accurately by likelihood decoding the two received signals.

We can also find that the performances of 1Tx, 2Rx scheme with MRC are better than those of 2Tx, 1Rx scheme. This is because if the transmitting power is distributed equally between two transmit antennas, transmitting power of each antenna will then be halved, which means that the output SNR decreases and coding gain of the system is weakened accordingly, then results in the decline of BER performances. In summary, according to results in Figure 4, information hiding system combined with space-time processing, whether transmit diversity or receive diversity, will have a better hiding performance than information hiding system in single input single output (SISO) system.

In Figure 5, the three curves represent different BER performances of secret data when space-time processing is absent, when Alamouti space-time coding is used and when receive diversity technique is used. We find that compared to the BER performances of secret data in SISO system, the BER performances of the schemes with space-time processing and MRC are much enhanced. The higher the SNR is, the better performance it can obtain.

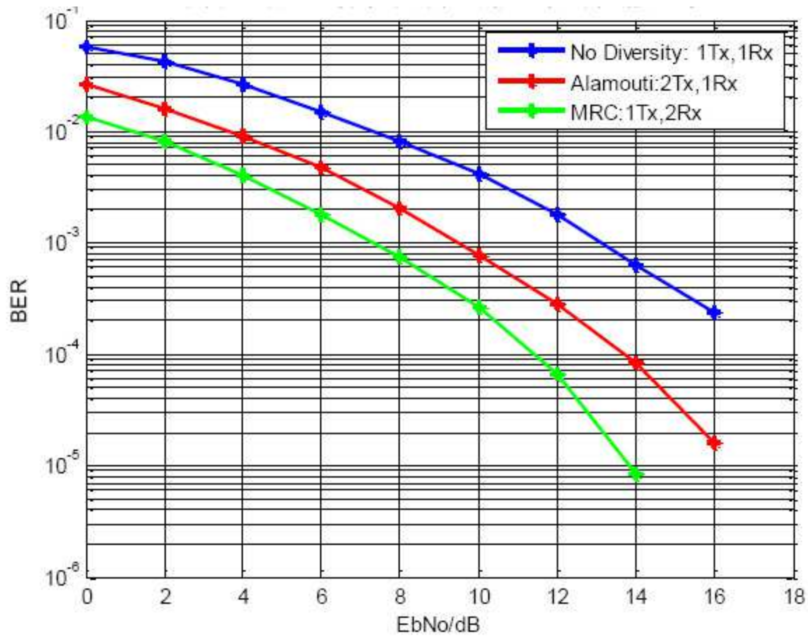


Figure 5. BER of secret data vs. SNR in multiple antenna system

4.2. **Transmitter diversity simulations.** Assume that the carrier image is 768K Bytes in size and based on (15,7,4) RS channel code, the secret image data is 19K Bytes in size and uses (31,21,2) BCH error correcting code. The modulation method is BPSK. P_T is the total power of transmitted signal and is normalized to 1. There is only one antenna in the receiver, while there are one to four antennas in the transmitter. The channel matrix coefficient is Rayleigh distribution, the channel SNR ranges from 5dB to 20dB. In Figure 6, the information hiding capacity in MIMO channel is presented. Here, 1×1 represents one transmitting antenna and one receiving antenna, 2×1 represents two transmitting antennas and one receiving antenna, and so on.

If the channel coding scheme, error correcting code, carrier data, secret data and channel condition are all the same, the information hiding capacities based on different diversity schemes in multiple antenna system can be calculated from equation (6). In Figure 6, y axis shows the embedding rate. When the carrier size and channel coding are known, y reflects the hiding capacity. The greater the y is, the more the secret data can be embedded in the multiple antenna system. From Figure 6 we also can find that if channel condition is the same and BPSK modulation is used, compared to SISO system, antenna diversity technique will effectively reduce the errors caused by channel interference and higher information hiding capacity ratio is obtained, i.e., the information hiding capacity will increase.

Moreover, information hiding capacity ratio will increase with the increase of antenna number. For example, in channel with 10dB SNR, the hiding capacity ratio of 1×1

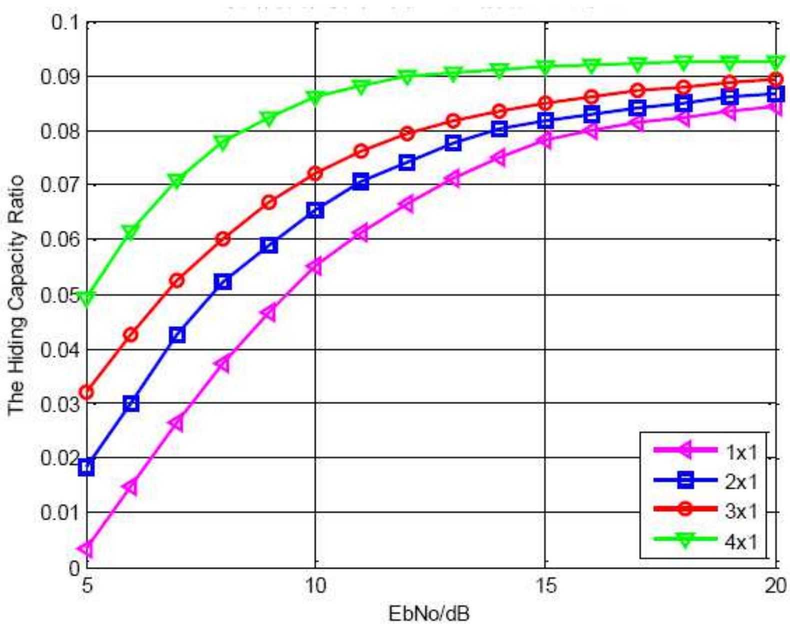


Figure 6. Hiding capacity ratios vs. SNR in transmit diversity simulation

antenna system is about 0.055, the hiding capacity ratio of 2×1 antennas system is about 0.065 while the hiding capacity ratio of 4×1 antennas system can reach 0.087. Based on the above simulated parameters, neglecting the effect of channel noise, the upper limit of hiding capacity ratio is about 0.0952, which represents the information hiding capacity ratio in ideal channels. However, in practical channels, noise and other interferences are unavoidable, thus, it's impossible for the actual information hiding capacity ratio to reach this value.

According to the tendency of the above curves, with the improvement of channel conditions, information hiding capacity ratio trends to be stable regardless of whether diversity techniques are used or not. There is a noticeable gap between increases because of different diversity gains. The larger the diversity gain, the higher information hiding capacity ratio can be obtained for low SNR cases. Consequently, in terrible channel conditions, multiple antenna diversity techniques can help information hiding systems to obtain better BER performance.

4.3. **MIMO technology simulations.** Based on equation (25), the upper threshold of information hiding based on channel coding is calculated while MIMO techniques are used. Assuming that the carrier data is the lena.tiff image in size of 768K bytes, carrier data uses $(15, 7, 4)$ RS channel code and secret data uses $(31, 21, 2)$ BCH code for preprocessing. The modulation method is BPSK, and the channel SNR ranges from 5dB to 20dB. The simulation results are shown in Figure 7.

In Figure 7, compared to SISO system or the other multiple antenna systems which include transmitter diversity only or receiver diversity only, MIMO technique can effectively reduce the errors caused by channel interference in the same channel conditions, thus enabling them to obtain larger information hiding capacity ratio.

For example, in a channel where the SNR is 10dB, the information hiding capacity ratio is about 0.055 in the system with only one transmitting antenna and one receiving antenna, while it is approximately 0.065 in the system with $n_R = 1, n_T = 2$ and 0.088 in the system with $n_R = 2, n_T = 2$. When two transmitting antennas and four receiving antennas are working in the system, the information hiding capacity ratio will reach the upper limit. As can be seen, channel error will be significantly improved with the increase of $N_T N_R$, which enables the information hiding system based on channel coding in MIMO systems to reach the upper limit of information hiding capacity.

Also in Figure 7, the hiding capacity ratio of 2×4 (2 Tx, 4Rx) will reach the maximum when $E_b N_o$ is about 10dB, while that of 1×2 (1 Tx, 2Rx) will reach the maximum when $E_b N_o$ reaches 20dB. Here, the exact SNR value for the hiding capacity ratio reaching the maximum will depend on different multiple antenna technologies and different channel models.

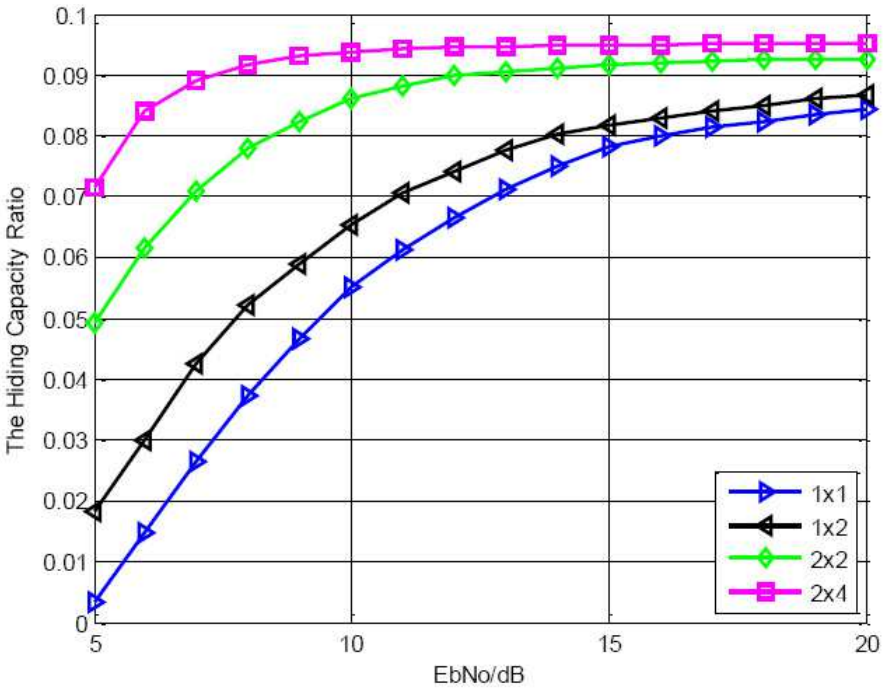


Figure 7. Hiding capacity radios vs. SNR in MIMO simulation

4.4. **Space-time coding simulations.** Assume that the carrier data is the image lena.tiff in size of 768K Bytes and based on $(15, 7, 4)$ RS channel code, the simulation results of space-time coding are shown in Figure 8.

The three curves in Figure 8 represent the different information hiding capacity ratios in SISO system, MIMO system with $n_R = 2, n_T = 1$ and multiple antenna system with Alamouti space-time coding. According to Figure 8, under the same conditions, information hiding capacity ratios in Alamouti space-time coding system are larger than those in SISO system. It can also be seen that, in the same condition, information hiding capacity ratio in Alamouti coding system with $n_R = 2, n_T = 1$ is slightly worse than that in $n_R = 1, n_T = 2$ system with MRC used. This is because, the transmitting power is distributed equally between two transmit antennas in Alamouti coding system, which results in loss of SNR, and thus leads to a gap in BER performance.

However, for a wireless terminal, processing power as well as other factors have limited the applications of receive diversity techniques. In order to improve the performance of MIMO wireless systems, combining transmitter diversity with space-time coding is more popular. Consequently, space-time coding techniques play an important role in improving of the performance of multiple antenna systems.

Here, we can also find that the information hiding capacity ratios in Figure 8 based on simulations are the same as those computed from equation (35), which are listed in Table 1 with SNR is 10dB or 20dB.

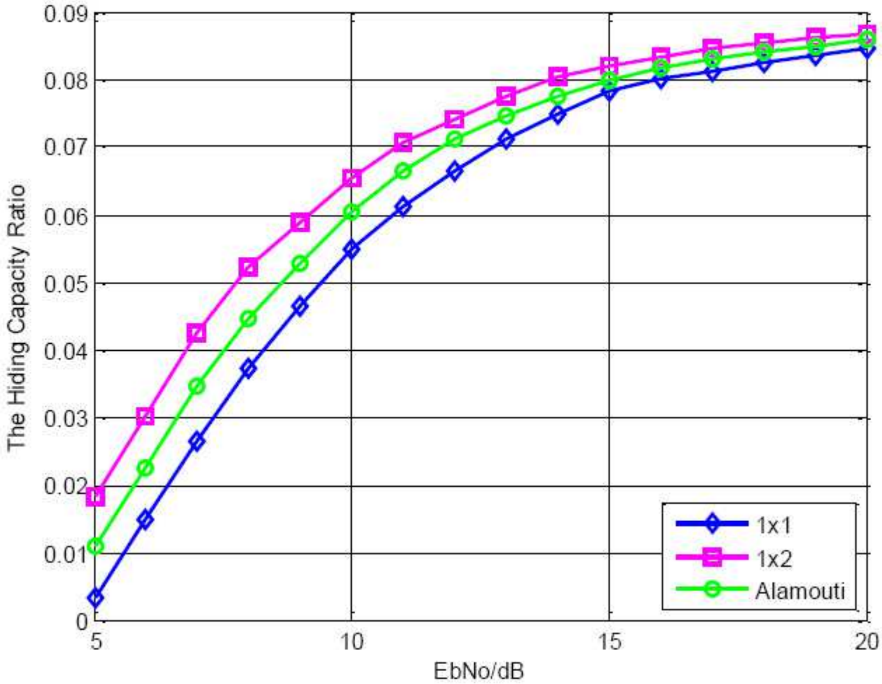


FIGURE 8. Hiding capacity ratios vs. SNR in Alamouti simulation

5. **Conclusion.** In this paper, the structure of information hiding system based on channel coding in multiple antenna system is built, the effects of transmitter diversity, receiver diversity, MIMO technology and space-time coding techniques on information hiding capacity are analyzed. According to the numerical analysis results and simulation results, both antenna diversity techniques and space-time coding techniques can reduce the errors caused by channel interference, thus indirectly increase the information hiding capacity in multiple antenna systems. Moreover, antenna diversity techniques and space-time coding techniques can reveal more advantages in information hiding capacity especially for low SNR cases. With the development of information hiding and channel coding techniques, information hiding in MIMO systems will certainly acquire broader development and application.

Acknowledgement. This work was supported in part by the national High Technology Research and Development Program of China (863 program) under grant No. 2013AA014001 and by the national Natural Science Foundation of China (NSFC) under grant No.61372103.

REFERENCES

[1] Y. Tew, and K. S. Wong, An overview of information hiding in H. 264/AVC compressed video, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 24, no. 2, pp. 305-319, 2014.
[2] M. Lu, and L. Q. Chen, Analysis of information hiding capacity in the multiple antenna coding channel system, *Journal of Nanjing University of Posts and Telecommunications (Natural Science)*, vol. 32, no. 5, pp. 6-11, 2012.
[3] H. T. Ma, X. W. Yi, and X. H. Wu, A capacity self-adaption information hiding algorithm based on RS code, *International Conference on Multisensor Fusion and Information Integration for Intelligent Systems (MFI)*, pp. 1-8, 2014.

[4] L. J. Kong, and Y. Xiao, Information hiding scheme based on LDPC coding, *The 8th International Conference on Signal Processing*, vol. 1, pp. 543-552, 2006.

[5] A. Valizadeh, and Z. J. Wang, An improved multiplicative spread spectrum embedding scheme for data hiding, *IEEE Trans. Information Forensics and Security*, vol. 7, no. 4, pp. 1127-1143, 2012.

[6] E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, Massive MIMO for next generation wireless systems, *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186-195, 2014.

[7] A. Akhlaq, A. I. Sulyman, and H. Hassanein, Performance analysis of relay-multiplexing scheme in cellular systems employing massive multiple-input multiple-output antennas, *IET Communications*, vol. 8, no. 10, pp. 1788-1799, 2014.

[8] J. J. Harmsen, and W. A. Pearlman, Capacity of steganographic channels, *IEEE Trans. Information Theory*, vol. 55, no. 4, pp. 1775-1792, 2009.

[9] Y. Xie, J. Li, and Y. L. Zhang, A high capacity information hiding method for webpage based on tag, *The Third International Conference on Digital Manufacturing and Automation (ICDMA)*, pp. 62-65, 2012.

[10] L. J. Hu, and R. D. Wang, Large capacity information hiding for H.264/AVC, *International Conference on Electronics, Communications and Control (ICECC)*, pp. 878-882, 2011.

[11] X. H. Yan, Information hiding capacity model based on error-correcting codes, *Computer Engineering*, vol. 36, no. 3, pp. 172-173, 2010.

[12] A. F. Coskun, and O. Kucur, Performance analysis of maximal-ratio transmission, *IEEE Trans. Vehicular Technology*, vol. 61, no. 3, pp. 1099-1108, 2012.

[13] G. C. Su, Research on downlink performance and capacity of distributed antennas system, *Master thesis*. Shanghai: Shanghai Jiao Tong University, 2010.

[14] W. Arita, and M. Saito, Novel receive diversity scheme using ESPAR antenna and arbitrary frequency band, *IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1-5, 2012.

[15] A. Paulraj, R. Nabar, and D. Gore, Introduction to Space-Time Wireless Communications, *Cambridge University Press*, 2008.

[16] D. Ben, C. Battikh, J. M. Kelif, and M. Coupechoux, Dynamic system performance of SISO, MISO, and MIMO Alamouti schemes, *IEEE Sarnoff Symposium*, PP. 1-5, 2011.

[17] N. Agarwal, and S. Nema, Performance analysis of Alamouti scheme in Rayleigh channel, *IEEE International Conference on Communication, Information, Computing Technology (ICCICT)*, pp. 1-6, 2012.