ENCRYPTED IMAGE TRANSMISSION OVER MIMO CHANNEL FOR SECURED COMMUNICATION USING COMPRESSIVE SENSING TECHNOLOGY

Dhivya K[1], Kannagi V[2], Sandhiya G[3], Muralikannan K[4]

[1,2,3]ECE, RMK College of Engg., and Technology,RSM Nagar, Puduvoyal, (India)

[4]Vanguard logistics, T.Nagar, Chennai, (India)

ABSTRACT

In wireless communication, the channel is characterized by multipath propagation due to scattering by different obstacles. Multiple Input Multiple Output (MIMO) channel which considers this multipath propagation offers significant increase in data throughput and link range without additional bandwidth or transmit power. With the availability of high data rates by MIMO channel, images can be transmitted with high reliability. An image is source coded by using Compressive Sensing (CS) algorithm where the input image is converted to bit streams. These bit streams are spatially multiplexed into four data streams which are transmitted simultaneously over the four antennas. The data streams are then channel coded by using 4-Quadrature Amplitude Modulation (4-QAM).Then unequal power allocation scheme is employed where each transmitting antenna gets different amount of power according to the data it transmits. The result is simulated using MATLAB. The results show that the unequal power allocation provides significant quality improvement than the any other technique. The result also reveals that Spatial diversity can be utilized more efficiently using Compressive Sensing.

Keywords: MIMO, Compressive Sensing, Unequal Power Allocation, Joint Source Channel Coding.

I. INTRODUCTION

In radio communication, **multiple-input and multiple-output**, or **MIMO**, is the use of multiple antennas at both the transmitter and receiver to improve communication performance. It is one of several forms of smart antenna technology. The terms input and output refers to the radio channel carrying the signal, not to the devices having antennas.

The core idea behind MIMO is that the signals sampled in the spatial domain at both ends are combined in such a way that they either create effective multiple parallel spatial data pipes or add diversity to improve the quality of the communication. The channel capacity of the MIMO channel depends upon the knowledge of the channel gain matrix or its distribution at the transmitter or at the receiver.

JSCC is the most commonly studied joint design problem for image and video communication in the literature. Another important joint design problem is that of transmission power allocation and optimization for image and video communication. The main goal for such problems is either to minimize the total distortion with a constraint on available transmission power, or to minimize the power usage with a constraint on maximum ―tolerable distortion.

In Spatial multiplexing, a high rate signal is split into multiple lower rate streams and each stream is transmitted from a different transmit antenna in the same frequency channel. If these signals arrive at the receiver antenna array with sufficiently different spatial signatures, the receiver can separate these streams into (almost) parallel channels. Spatial multiplexing is a very powerful technique for increasing channel capacity at higher signal-to-noise ratios (SNR).

Compressive sensing (CS) is an emerging sampling paradigm. Sparsity and incoherence are two fundamental concepts in the CS, which involve with the following three major aspects: sparse representation, random measurements taking and signal recovery via $\ell 1$ minimization. Compressed sensing takes advantage of the redundancy in many of interesting signals.

In particular, many signals are sparse, that is, they contain many coefficients close to or equal to zero, when represented in some domain.[7] This is the same insight used in many forms of lossy compression. Compressed sensing typically starts with taking a weighted linear combination of samples also called compressive measurements in a basis different from the basis in which the signal is known to be sparse.

In [4], Modestino *et al* presented joint source channel coding technique for images where mean square error (MSE) is used to find the distortion. This demonstrated significant image quality improvement using efficient channel coding. In [22], Lu *et al* proposed a power minimization method with a constraint on total allowable distortion. This method showed around 3.5 dB PSNR gain when compared to conventional techniques.

In [23], Appadwedula *et al*. presented a power optimization method where the source coder, channel coder and power consumption were jointly optimized. In [24], Yu *et al.* proposed an energy optimizing scheme for image transmission over wireless sensor networks. With the constraint on total distortion, the source coding, the channel coding rate and the transmission power levels are minimized.

In [7], Ji *et al.* developed a power optimization method for transmission of MPEG-4 bit streams. In this method, total distortion was minimized by power-efficient assignment of scalable source to spatial sub channels with a constraint on total transmit power. Their scheme showed a PSNR gain of around 2.5 dB as compared to different nonoptimal schemes.

II. SYSTEM DESIGN

The system design and the description of the components present in this system are given below.

2.1 Source Coding Design

The original gray image is first encrypted as a set of coefficients by a secret orthogonal transform, and the network provider compresses the encrypted coefficients into a small amount of measurement data using a linear operation. Due to the sparsity of natural image in conventional transform domain, the compressive sensing method can be introduced to compress the data of the encrypted images.

2.2 Spatial Multiplexing

After compression of the image using Compressive sensing, the bitstream is passed to the spatial multiplexing (SM) block. The SM block divides this bitstream into four equal length streams, since there are four transmit antennas. Streams are formed in order of importance, with stream number 1 being the most important and stream number four being the least important. These streams are then passed to the power optimization block for unequal power allocation. At the receiver, the multiplexer/combiner combines these streams into a single stream and passes it to the GPSR block for reconstruction of the original image.

2.3 Channel Model

Four transmit and four receive antennas are used in this model for the transmission of JPEG compressed bit streams. The channel matrix **H** is a 4 X 4 matrix whose entries form an i.i.d. Gaussian collection with zero-mean, independent real and imaginary parts, each with variance 1/2. Four-Quadrature amplitude modulation (4-QAM) is used for modulating the bitstream.

2.4 MMSE Receiver

Mean-squared error (MMSE) receiver is used to decode the spatially multiplexed bitstream. The MMSE receiver is a linear receiver, i.e., it separates the transmitted data streams and then independently decodes each stream. Without loss of generality, the symbol period can be normalized to 1 to simplify the relationship between transmit power and energy. Also, it can be assumed that the noise covariance matrix is the Identity matrix I_4. Hence, the transmit power is equal to signal-to-noise ratio (SNR) per symbol during any symbol period. Then, the received signal vector can be written as

$$Y = HX_n s + n$$

where Y is the received 4 x 1 signal vector, s the 4 x 1transmit signal vector, and n is the 4 x 1 zero mean circularly symmetric complex Gaussian noise vector with covariance matrix I_4.

III. IMAGE ENCRYPTION AND COMPRESSION

The size of the input image is adjusted so that its rows and columns are in multiples of 32. The image is divided into non- overlapping blocks of size 32 x 32. For each block the average value of the pixel is calculated. In each and every block the zero mean version of the pixel is calculated. The pixels in the block are then arranged in the form of vector P. An orthogonal matrix H of size 1024 x 1024 is generated. The orthogonal matrix is multiplied with the vector to generate a column vector Q. Encrypt the average value using any secret key. For compressing the encrypted image a compression matrix of size 1024 x 1024 is generated whose rows are mutually orthogonal. The compression matrix is multiplied with the vector Q which results in compressed data.

IV. UNEQUAL POWER ALLOCATION

All parts of the compressed image are not equally important. Only few parts have significant importance to image quality. So, more important streams should be transmitted with more protection from errors as compared to less important streams. One way to achieve this is to transmit different streams with unequal transmit power with more important streams being transmitted with more power and less important streams with lesser power, without violating the total transmit power constraint.

At any given instant, the channel from a particular transmit antenna to the receive antennas might be better than the channel corresponding to the remaining transmit antennas. In fact, the channels from different transmit antennas to the receive antennas are very likely to be different at different times. Therefore, a natural idea is to transmit more important streams from ―more reliable‖ transmit antennas and less important streams from

―less reliable‖ antennas. This makes sense intuitively since less power will be required by the most important stream if it is being transmitted from the best antenna as compared to that of a random antenna.

Hence, more power can be allocated to less important streams resulting in further reduction of overall distortion. Since the channel stays constant for a block of symbols, and then changes, an antenna selection process needs to be performed for each block of symbols in real time. For compressing the encrypted image a compression matrix of size 1024 x 1024 is generated whose rows are mutually orthogonal. The compression matrix is multiplied with the vector Q which results in compressed data.

4.1 Power Allocation Algorithm

For real-time applications, it is necessary that the power optimization procedure should be computationally non-intensive. The number of computations can be significantly reduced by devising simple suboptimal algorithms that divide the original problem into optimization problem with fewer numbers of variables, without imposing a large penalty on performance. Based on this idea, a suboptimal algorithm for the power allocation problem is developed. This algorithm quantizes the transmit power for different streams and essentially breaks down the four variable optimization problem into an iterative two variable optimization problem. The algorithm is summarized below.

Step 1: Initialize the values as k=1, m=1, E_A=0, $MSE_{min} = \infty$ and $\Delta_1 = E_s / M_1$.

Step 2**:** For k=1, …,4, find the following.

Step 3**:** $X_{k,n} = E_s - m * \Delta_k - E_A$.

$X_{k+1,n} = .. = X_{4,n} = m*\Delta_k/(4-k)$.

Step 4**:** Find the MSE of X_n .

Step 5: If $MSE(X_n) < MSE_{min}$

Then $MSE_{min} = MSE(X_n)$,

$X_{min} = X_{k,n}$, m=m+1.

Step 6: If $m < M_k$ then

$X_{k,n} = X_{min}$ and k=k+1, m=1,

$E_A = E_A + 1$.

Step 7: If k < 4, go to step 1 else MSE_{min} has the minimum value of MSE and has the corresponding transmit power.

This algorithm uses the fact that the received SINR for a more important stream needs to be greater than the received SINR for a less important stream to minimize the distortion.

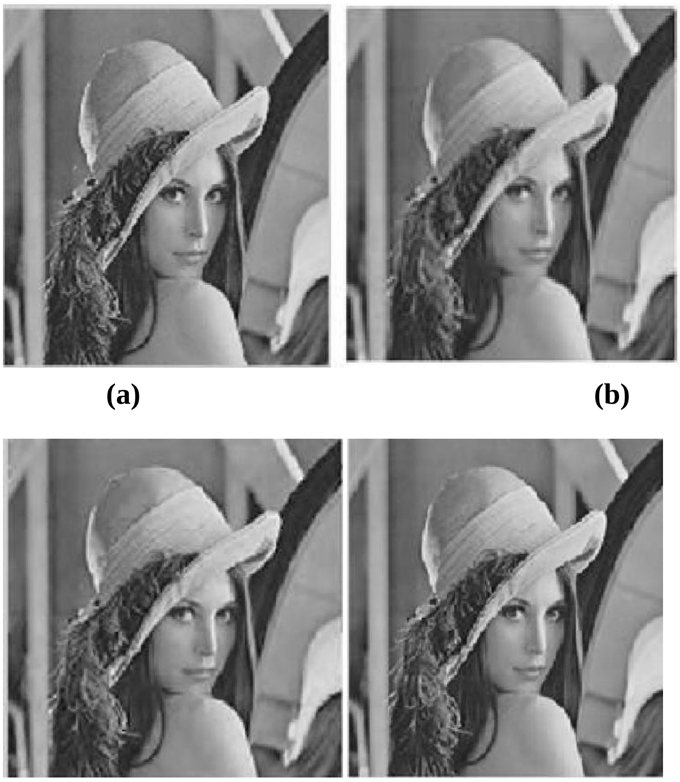
Using this fact, this algorithm do not compute distortion at all quantized power levels.

V. SIMULATION RESULTS AND DISCUSSION

The model parameters, namely the unquantized coefficient mean and variance, the quantization error mean and variance, were found using the original unquantized image and the quantization matrix. The values of M_1 =30, M_2= 20, M_3=M_4= 10 were numbers of quantized power levels that were used for different streams for the suboptimal power allocation method.MSE was converted to PSNR using the simple relation

$$PSNR = 10 \log_{10}(255^2/MSE),$$

Different streams for the EPA scheme with antenna selection also have different BERs. The average BER of all these streams is approximately the same, however, as that of the EPA scheme without antenna selection, and sequential JPEG with EPA. Also note that EPA with antenna selection performs better in terms of PSNR as compared to EPA without antenna selection (for progressive JPEG) at all points, and better than EPA for sequential JPEG for medium to high SNR range. This shows that the idea of antenna selection provides better performance than randomly assigning transmit antennas to different streams.



(a) **(b)**

(c) **(d)**

Fig.1.(a) Original image (b) Reconstructed image using JPEG (c) Reconstructed image using JPEG 2000 (d) Reconstructed image using GPSR

From the simulated results, reconstructed image using Gradient projection for sparse reconstruction (GPSR) has better quality than reconstructing using existing JPEG and JPEG 2000 compression and reconstruction algorithms.

The amount of distortion predicted by the distortion model during the optimization procedure is very close (within 1 dB) to that of the actual amount obtained via transmission simulations. This method can also be extended to power constrained efficient video transmission over MIMO systems using our distortion model for video.

VI. CONCLUSION

An image is encrypted using a secret key where the input image is converted to bit streams and then the encrypted bit streams are compressed using Compressive Sensing (CS) algorithm. These compressed bit streams are spatially multiplexed into four data streams which are transmitted simultaneously over the four antennas.

The data streams are then channel coded by using 4-Quadrature Amplitude Modulation (4-QAM).Then unequal power allocation scheme is employed where each transmitting antenna gets different amount of power according to the data it transmits. The overall transmit power is kept constant at any given instant. Results show that the amount of data transmitted using CS technique is less when compared with the traditional JPEG techniques. The result also shows that the quality of the reconstructed image is better using GPSR technique than other techniques. The unequal power allocation scheme provides significant gains in terms of PSNR over various equal power allocation schemes. These results indicate that significant quality gains can be achieved if the source statistics are taken into account while designing transmission schemes without imposing any penalty on resources. The result also reveals that the spatial diversity order of the compressive sensed data is more than the JPEG family compressed data.

Table I

Comparison of parameters

PARA METER	**JPEG**	**JPEG 2000**	**CS**
CR	8.0570	27.6074	49.0456
MSE	54.0366	24.3232	19.2639
PSNR	30.8039	34.2705	40.5326

Table II

Comparison of no. Of bits for different compression schemes

NAME OF THE IMAGE	**SIZE OF THE IMAGE**		**OUTPUT BITS FOR JPEG**	**OUTPUT BITS FOR JPEG 2000**	**OUTPUT BITS FOR CS**
Lena.png	256 x 256		15498	4602	2594
Barbara.png	256 x 256		18616	4626	2598
Cameraman.tif	256 x 256		16795	5594	2636

REFERENCES

[1]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, ―On Compressing Encrypted Data,‖ *IEEE Trans. Signal Processing*, 52(10), pp. 2992–3006, 2004.

[2]. A. J. Goldsmith and M. Effros, ―Joint design of fixed-rate source codes and multiresolution channel codes ,‖ *IEEE Trans. Commun.*, vol.46, no.10, pp. 1301–1312, Oct. 1998.

[3]. D. L. Donoho, ‗‗Compressed Sensing,'' *IEEE Trans. Information Theory*, 52(4), pp. 1289--1306, 2006.

[4]. N. Farvardin and V. Vaishampayan, ―Optimal quantizer design for noisy channels: An approach to combined source-channel coding, *IEEE Trans. Inf. Theory*, vol. IT-33, no. 11, pp. 827–838, Nov. 1987.

[5]. P. Sherwood and K. Zeger, ―Error protection for progressive image transmission over memoryless and fading channels, *IEEE Trans Commun.*, vol. 46, no. 12, pp. 1555–1559, Dec. 1998.

[6]. J. W. Modestino and D. G. Daut, ―Combined source-channel coding of images, *IEEE Trans. Commun.*, vol. COM-27, no. 11, pp. 1644–1659, Nov. 1979.

[7]. [7] J. W. Modestino, D. G. Daut, and A. L. Vickers, ―Combined Source channel coding of images using the block cosine transform.*IEEE.Trans. Commun.*, vol. COM-29, pp. 1261–1274, Sep. 1981.

[8]. V. Chande and N. Farvardin, ―Progressive transmission of images over memoryless noisy channels, *IEEE J. Sel. Areas Commun.*, vol. 18, no. 6, pp. 850–860, Jun. 2000.

[9]. P. G. Sherwood and K. Zeger, Progressive image coding for noisy channels,‖ *IEEE Signal Process. Lett.*, vol. 4, no. 7, pp. 189–191, Jul.1997.

[10]. [10] D. Donoho and Y. Tsaig, Extensions of compressed sensing,‖ *Signal Process.*, vol. 86, no. 3, pp. 549–571, 2006.

[11]. [11] E. Candès and J. Romberg, ―Practical signal recovery from random projections,‖ in *Proc. SPIE Conf. 5914 Wavelet Appl. Signal Image Process. XI*, 2004.

[12]. Y. Eisenberg, C. Luna, T. Pappas, R. Berry, and A. Katsaggelos, ―Joint Source coding and transmission power management for energy efficient wireless video communications, *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 411–424, Jun. 2002.

[13]. [13] L. Atzori, ―Transmission of JPEG2000 images over wireless channels with unequal power distribution,‖ *IEEE Trans. Consum. Electron.*, vol. 49, no. 11, pp. 883–888, Nov. 2003.

[14]. [14] H. Zheng and K. Liu, ―The subband modulation: A joint power and rate allocation frameworkfor subband image and video transmission, *IEEE Trans. Circuits Syst. Video Technol.*, vol. 9, no. 5, pp. 823–838, May 1999.

[15]. [15] Q. Zhang, W. Zhu, Z. Ji, and Y.-Q. Zhang, ―A power-optimized joint source channel coding for scalable videostreaming over wireless channel, in *Proc. IEEE Int. Symp. Circuits and Systems*, 2001, vol. 5, 137–140.

[16]. Z. Ji, Q. Zhang, W. Zhu, and Y.-Q. Zhang, ―End-to-end power- Optimized video communication over wirelesschannels, in *Proc. IEEE 4th Workshop Multimedia Signal Processing*, 2001, pp. 447–452.

[17]. H. Jafarkhani, H. Yousefi'zadeh, and M. Moshfeghi, ―Power optimization of memoryless wireless media systems with space-time block codes, in *Proc. Global Telecommunications Conf.*, 2003, vol. 1, pp.123–127.

[18]. M. F. Sabir, H. R. Sheikh, R. W. Heath, Jr., and A. C. Bovik, ―A joint source-channel distortion model for JPEG comrpessed images, *IEEE Trans. Image Process.*, vol. 15, pp. 1349–1364, 2006.