Block Mean Modulation: An Effective and Robust Image Steganographic Technique in the Spatial Domain

A Nagalinga Rajan
Research scholar
Manonmaniam Sundaranar University
Tirunelveli

P Eswaran
Assistant Professor
Alagappa University
Karaikudi

R Sunder
Research Scholar
Manonmaniam Sundaranar University
Tirunelveli

S Poonkuntran
Assistant Professor
Velammal College of Engineering and Technology
Madurai

ABSTRACT
Image steganography is one of the emerging techniques for secret communication in the digital age. In order to have effective secret communication through image steganography, data hiding must be robust to image transformations and effective against analysis techniques. This paper proposes a novel spatial domain data hiding technique in which the secret message is embedded in the quantized mean of image blocks. The experimental results show that the message is preserved after applying common image modifications including jpeg compression, resizing and additive noise to some extent. The block size and quantization factor are optimized through trial and error. The mean of the intensity values in a block is the same as the DC coefficient of the DCT of the block. The effectiveness against common steganalysis methods is also established.

General Terms
Information hiding, Steganography

Keywords
Information hiding, Steganography, Image transformations, JPEG compression, Modulation, Steganalysis

1. INTRODUCTION
Steganography provides the means to secret communication where not only the message is hidden but also the very presence of the message is hidden [1]. This allows individuals to exchange secret communication without raising alarm of a presumably hostile censorship authority. Hiding in images is preferable due to its high embedding capacity as a result of redundancy in digital image representations [2] and increased stealth due to the presence of massive amounts of images present in the internet [1].

Generally a good data hiding technique must preserve the visual similarity of the image and guard against detection by steganalysis methods. The message must be preserved when the image is transmitted through a communication channel. An application in which steganography is built seamlessly into a high throughput communication medium such as a TV channel broadcast is considered. A method that is robust to common image modifications is needed in this case [1]. Message integrity can be sacrificed a little if it can be recovered through redundancies built into the system such as error correcting codes [3]. This paper proposes a novel data hiding algorithm in the spatial domain of Images for these types of applications.

2. REVIEW OF STEGANOGRAPHIC METHODS
Several steganographic methods have been proposed in the last few decades. The simplest technique called Least Significant Bit (LSB) substitution simply replaces the least significant bits of the cover image with the secret message [4]. But it is not effective against steganalysis techniques such as the pair of values analysis by Westman & Pfitzmann [5], RS-Steganalysis by Fridrich et al [6] and primary sets technique introduced by Dumitrescu et al [7]. A simple but important modification known as LSB matching [8] consists of changing the LSB of the cover to match the secret message. In order to change the LSB it randomly chooses to add either +1 or -1. LSB matching can be detected by the center of mass (COM) of the histogram characteristic function (HCF) introduced by Harmsen et al [9] and also more effectively by adjacency HCF COM by Ker [10]. Mielikainen has proposed the LSB matching revisited [11] which improved the effectiveness against analysis by minimizing the distortion of the cover image. Effective steganalysis of this technique remains a challenge although some success has been achieved in the case of consecutive pixel pairs by Shunquan Tan [12]. All the methods described above are substitution methods and do not provide message integrity when the medium undergoes common image processing transformations. The LSBs are very sensitive to simple transformations such as JPEG compression and noise addition [4].

Several transform domain techniques are also proposed where the message bits are hidden in the DCT coefficients. Some of the techniques that fall under this category are F5 [13], Outguess [14], and JSteg [15] etc. In addition to these model based techniques, spread spectrum based techniques etc. are also widely used [1].

In 2004, Michael Buchanan proposed creating a robust form of steganography called STEM which is a DCT transform domain technique [16].

Three basic requirements are important in designing a steganographic technique [1]. They are as follows:

1) Embedding capacity

The technique must be able to transmit as much information as possible in a given cover size

2) Robustness to transformation

The message must be preserved when the medium undergoes processing such as jpeg compression, resizing and noise addition.

3) Effectiveness against steganalysis

The method must provide resistance to simple steganalysis that can be applied on the medium.

In order to satisfy these requirements this paper introduces the quantization of mean value of Image blocks. The method is explained in detail in section 3; the characteristics of the method are presented in section 4 along with experimental results. Then conclusion is presented with some discussion on future work in section 5.

3. PROPOSED METHOD

Let I be the cover grayscale image of size m × n. A statistical quantity that is preserved in JPEG compression is needed. Since JPEG compression preserves low frequencies and affects only the higher frequencies [17] the mean being the lowest frequency, is selected to be such a quantity. Also JPEG compression acts on every 8 × 8 block [17]. Therefore the image I is partitioned into distinct blocks of size equal to s1 x s2. The mean of each block is taken to hold a bit of the secret message.

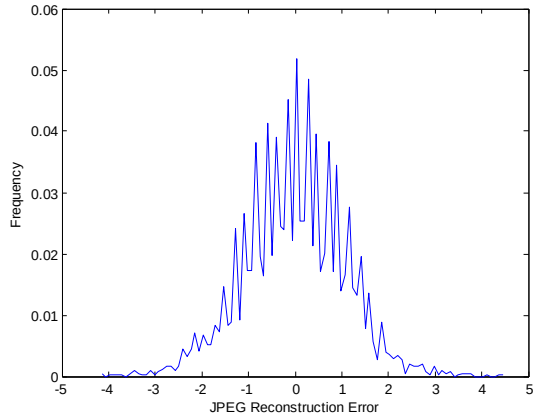


Figure 1 Distribution of JPEG Reconstruction Error

In Figure 1 the histogram of error in reconstruction of mean of blocks of size 4 × 4 and the compression quality of 50% is shown. From the figure, it is clear that the message can be preserved if the secret bit is stored after quantizing the mean with a factor of 5 or above.

In image resizing, the mean of blocks is preserved better than in JPEG compression if the number of divisions along the rows and columns is fixed.

Based on these observations the following method is proposed.

3.1 Secret Embedding Algorithm

1) Divide I into distinct blocks b_i of size $s_1 \times s_2$. The division is made such that there are r blocks per row and c blocks per column. The values of r and c are fixed so that the secret is preserved even if the image size and aspect ratio are altered.

2) Calculate the mean value of the elements in each block m_i

3) Embed the secret message bit smb_i to get the new mean in the following procedure. Here q is the quantization factor.

Calculate s = mod (floor (m_i/q), 2) If s is equal to smb_i, then change m_i to q*floor (m_i/q) +q/2. There are two options. It can be changed to q*(floor (m_i/q)-1) +q/2 or q*(floor (m_i/q) +1) +q/2. The one which is closer to m_i is chosen to minimize distortion. The two choices are equally likely and in this sense it is like LSB matching. In case the change causes an overflow or underflow of 8 bits then the other choice is taken. Let Δ denote the value to be added to m_i.

4) The values in the block have to be changed such that the mean works out to the new value. The value Δ*p*q is distributed among the p*q elements of the block. A share is added to each element proportional to its intensity value i.e., the share added to the j^{th} element b_{ij} is

$$\Delta pq \left(\frac{b_{ij}}{\sum_k b_{ik}}\right) \quad \ldots \quad (1)$$

The advantage in doing so is that the added signal acts as a multiplicative noise and less like an additive noise. Most steganalysis algorithms assume that the embedding is an additive noise and they detect its presence. By this distribution of mean change such steganalysis can be defeated.

3.2 Secret Extraction Algorithm

The image is divided into blocks so that there are r blocks per row and c blocks per column. The mean is calculated and the secret bit is read as

$$smb_i = \left\lfloor \frac{m_i}{q} \right\rfloor modulo\ 2 \quad \ldots \quad (2)$$

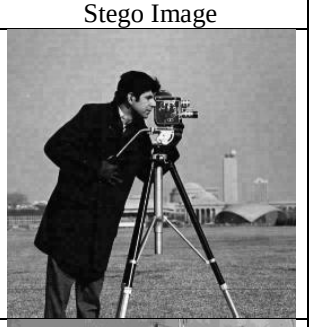
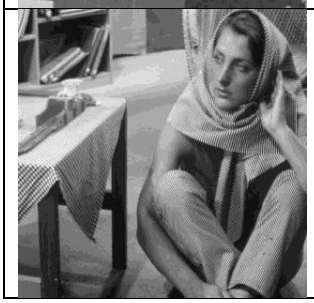
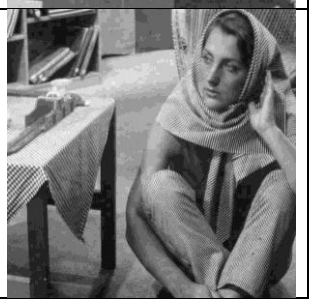
4. ANALYSIS AND VALIDATION

In the following subsections the results of experiments are shown along with the associated analysis. The experiments are conducted on a database comprising of 100 test images. The image results presented in this paper are from the following four test image shown in table 1. Table 2 shows the cover and stego images respectively.

Table 1 Test Images

	Image name	Image type	Size
1	Cameraman	Tif	256 × 256
2	Boats	pgm	512 × 512
3	House	pgm	512 × 512
4	Barbara	pgm	512 × 512

Table 2 Comparison of cover and stego images

Cover Image	Stego Image
	
	
	
	

4.1 Robustness against JPEG compression

JPEG compression involves the following steps. The image is converted to another color space, typically the YCbCr color space [18]. Then it is separated into 8 x 8 blocks and each block is transformed to discrete cosine transform (DCT) domain. Then the coefficients are quantized with different integers. The lower frequency coefficients are quantized with a smaller integer so that the loss is minimal and the higher frequencies are quantized with large integers and hence higher loss. The quantized coefficients are arithmetic encoded with run level encoding of zeros giving compression [17, 18].

The mean of a block's intensity corresponds to the low frequency or the DC component. Hence it is usually preserved in the compression. Experiments are conducted with different images and the accuracy of reconstruction of message as the quality of compression is varied is studied.

In Figure 2, the effect of JPEG compression on message integrity is shown. The block size is set to be 4 × 4 and q is set to be 5. From the figure it can be seen that these settings yield less than 5% error for quality greater than 50%. The error rates are prohibitively higher for lesser qualities of compression. The error of 5% is deemed reasonable because the redundancies such as error correcting codes can be used to rectify the loss of message bits.

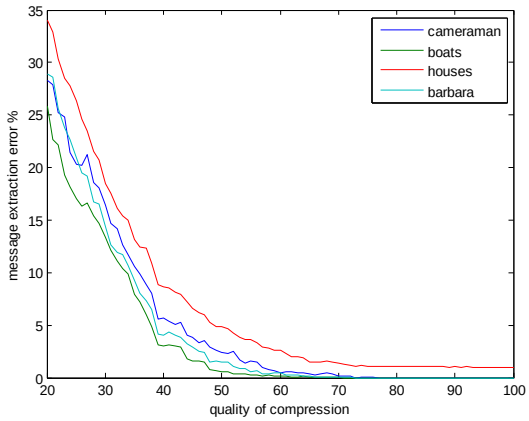


Figure 2 Impact of JPEG compression on message integrity

4.2 Robustness against Image Resizing

The hidden message is resilient to image resizing and can be recovered if the number of blocks along row and column is kept fixed. To study the effects of image resizing on the message integrity experiments are conducted with various test images and the error in message reconstruction versus the factor of resizing is plotted. Here aspect preservation is assumed but is not a necessary condition for the method.

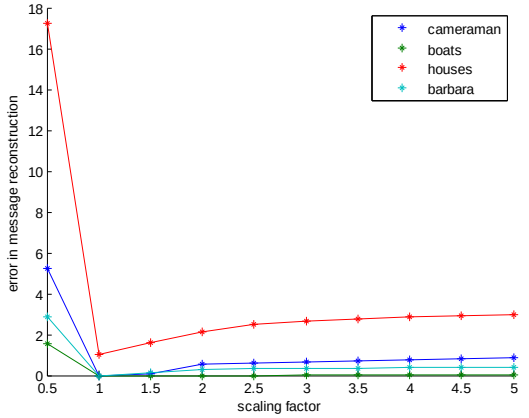


Figure 3 Effect of Resizing on Message Integrity

The factors are taken such that the blocks retain their integral size status. Otherwise information will be lost in the fractions of rows and columns. Here factors which are multiples of 0.5 are taken. All the images taken as the test cover images have even number of rows and columns. The block size is taken as 4 x 4 for the embedding and 4f x 4f for the extraction, where f is the resizing factor and q is taken to be 5. Naturally the message preservation is better in image upsizing but when the image is downsized there is a higher loss of message because there are fewer elements in each block to maintain the mean

to the correct level. In upsizing the maximum error level of 5 % is maintained (ref figure 5).

4.3 Robustness against additive noise

Additive Gaussian noise is added to the stego image and the integrity of the message is tested. Since additive noise with zero mean is usually the common form of noise in image transmission other than impulse noise, it is noted that the mean of a block is not perturbed greatly with zero mean additive noise. On the other hand impulse noises will displace the mean significantly which should be handled by a filter and since the secret channel is encoded as a multiplicative noise, it must remain intact through the impulse denoising procedure.

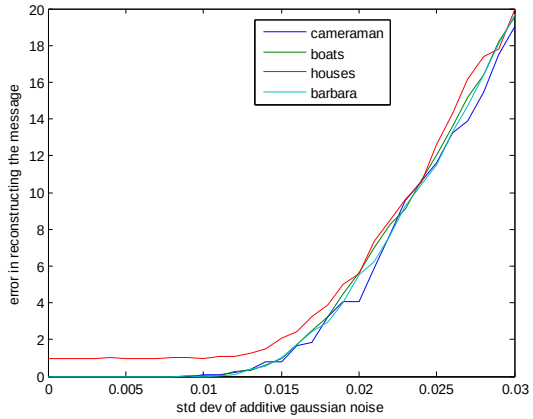


Figure 4 Impact of additive gaussian noise on Message Integrity

When impulse noise is involved, a filter based impulse noise removal method can recover the message hidden in the image without damaging it too much. This is demonstrated using salt & pepper noise and median filtering on the stego image in Figure 5.

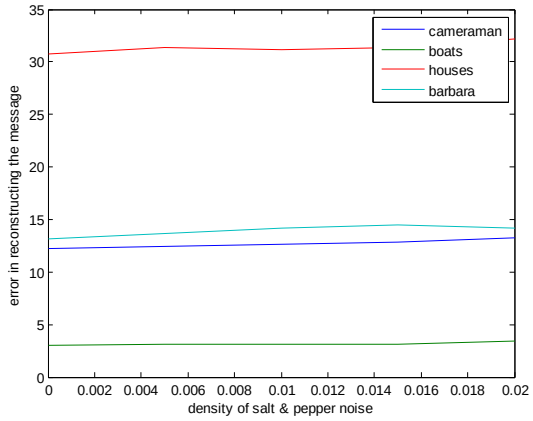


Figure 5 Impact of Salt & Pepper noise on Message Integrity

The performance leaves much to be desired. Working with the median instead of mean may overcome impulse noise but will not provide robustness against JPEG compression.

4.4 Effectiveness against adj-HCF-COM detector

The breakthrough in LSB matching steganalysis came in the form of Harmsen's HCF COM detector [9]. The method is designed to work with any steganographic technique which can be modeled as additive noise. HCF refers to the histogram characteristic function and COM refers to the center of mass. For a stego image with histogram H1[k], k =0,1,2…,255 the HCF COM is calculated as

$$C_1(H_1[k]) = \frac{\sum_{i=0}^{n} i|H_1[i]|}{\sum_{i=0}^{n}|H_1[i]|} \quad \ldots \quad (3)$$

Ker [10] improved the detection accuracy by combining calibration by down sampling with it and modifying the detector to work with adjacency histogram H2[k1,k2]. This ADJ-HCF-COM is calculated by

$$C_2(H_2[k]) = \frac{\sum_{i,j=0}^{n}(i+j)|H_2[i]|}{\sum_{i,j=0}^{n}|H_2[i,j]|} \quad \ldots \quad (4)$$

The ratio of C2 of an image to that of the calibrated image obtained by down sampling detects the presence of a secret message. Since the stego noise is distributed in a manner proportional to the intensity of the pixels the efficiency of ADJ-HCF-COM can be significantly reduced.

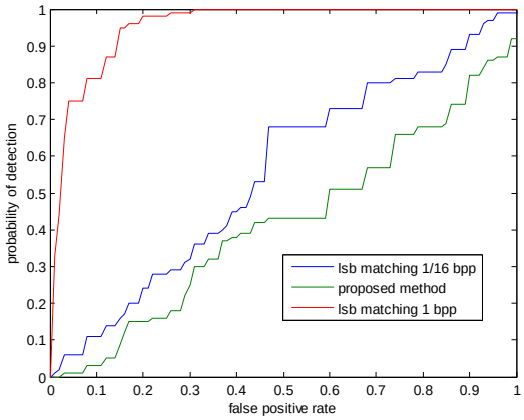


Figure 6 ROC curves for LSB matching, proposed method

The ROC curves for the proposed method is shown in Figure 6 along with the curves for LSB matching with the equivalent embedding rate of 1/16 bpp. The parameters used are block size of 4 × 4 and q = 5.

4.5 Parameter Selection

The parameters involved in the proposed method are block sizes $s_1 \times s_2$ and the quantization factor q. A higher q improves message integrity but also causes more distortion. It is seen through experiments that q can be set to 5 if up to 5% error in message reconstruction is tolerated.

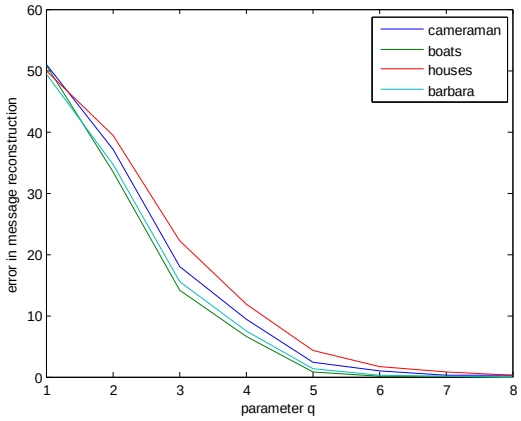


Figure 7 Impact of q on Message integrity

The plots of Figure 7 show the error in reconstruction of message as the parameter q is varied in which the stego image goes through JPEG compression of quality factor 50.

Higher block sizes increase message integrity but reduces the embedding capacity. It can be shown that for JPEG resilience in quality factor 50 %, the block size of 4 x 4 is optimal. Block sizes greater than 4 x 4 give message reconstruction error less than 5 %. Block size of 1 reduces the method to LSB embedding with quantization modulation and it can be clearly seen from Figure 8, that it is not robust to JPEG compression.

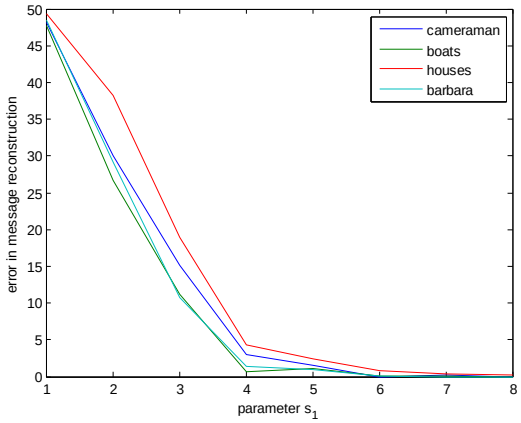


Figure 8 Impact of block size on message integrity

In the proposed method q is selected to be 5 and block sizes to be 4 x 4 with design choice of maximum allowable error in reconstruction of less than 5%.This type of embedding results in a stego image with Peak Signal to Noise Ratio (PSNR) around 40.

Table 3 PSNR of embedding

Cameraman	38.73
Boats	42.98
Houses	40.52
Barbara	40.89

4.6 Embedding in the DCT domain

A brief investigation into the possibility of embedding the message in the DCT domain is presented. Through experiments and insight, embedding in the DC coefficient is preferable to embedding in the AC coefficients. It also makes sense to perform DCT on 8 × 8 blocks. The parameter q has to be sufficiently large and it is experimentally fixed at about 20 where the error in recovered message is less than 5%. In Figure 9 some examples of stego images are presented and the PSNR values are shown in Table 4. Using a large quantization factor creates clearly visible artifacts and reduces the stealth provided by the method.

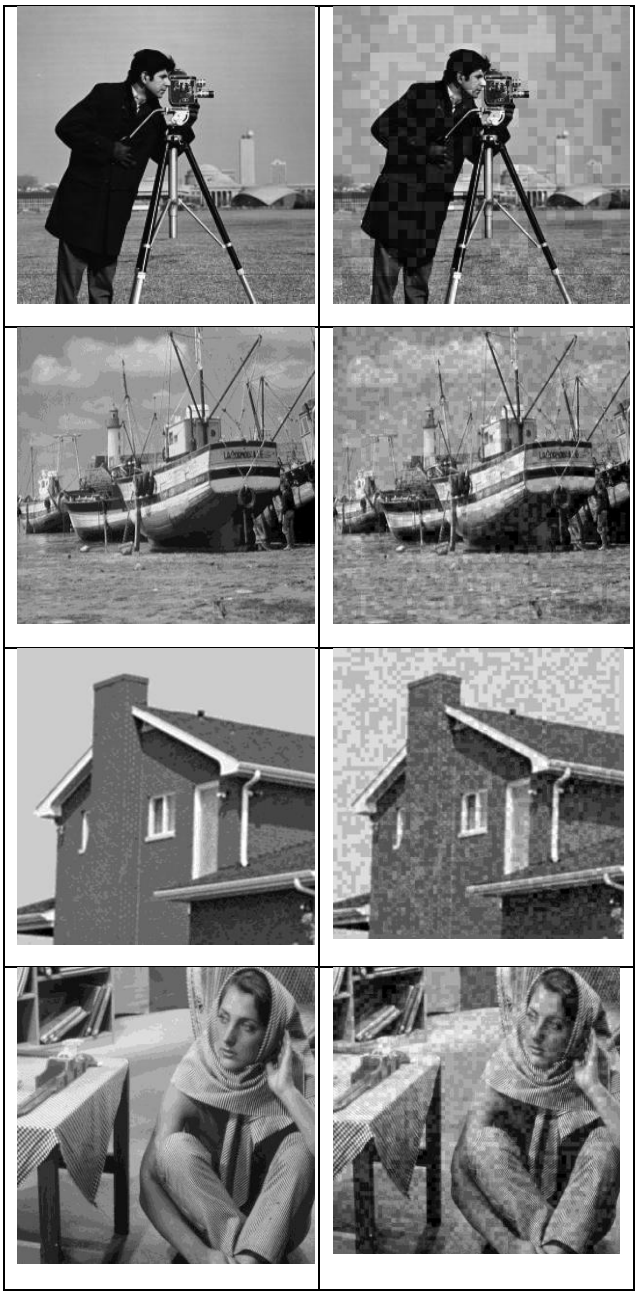


Figure 9 Stego Images with Embedding in DC coefficient (q = 20)

Table 4 PSNR values

Cameraman	31.40
Boats	35.06
Houses	30.10
Barbara	32.11

4.7 Improving embedding capacity

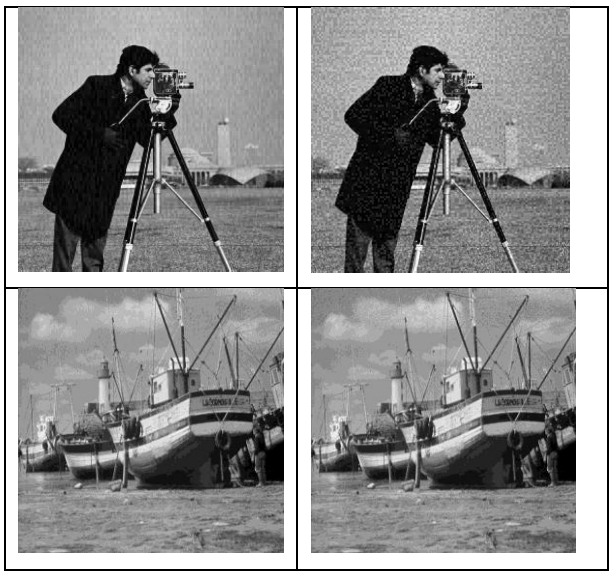
Using a block size of 4×4, 1/16 bits per pixel (BPP) is achieved. In this section a brief discussion on a possible modification which will improve the capacity is presented. Consider the 4×4 block and divide it into 4 parts of 2×2 contiguous parts and sum up each part. Then combine the four sum values with different linear coefficients to get four differently weighted means. Let s1, s2, s3, s4 be the four sums then the different weighted means are given by

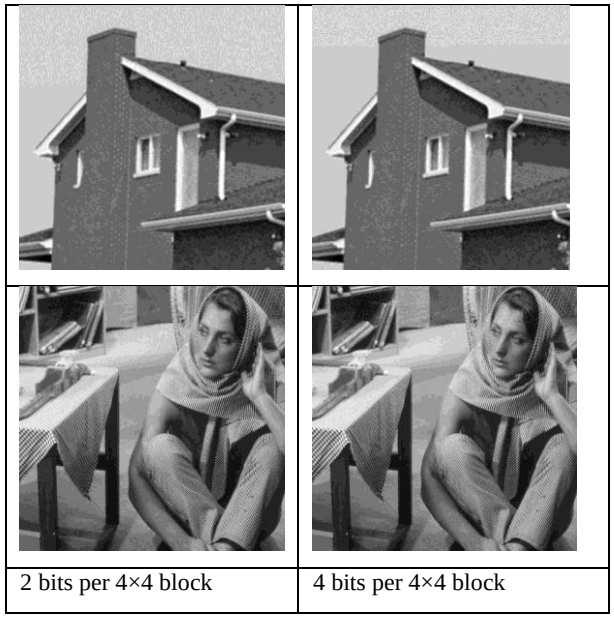
$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{bmatrix} = \begin{bmatrix} v & 1 & 1 & 1 \\ 1 & v & 1 & 1 \\ 1 & 1 & v & 1 \\ 1 & 1 & 1 & v \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} \quad \ldots \quad (5)$$

These means are modulated with four bits of message data thereby achieving an embedding rate of 1/4 Bits per pixel. After updating the means the above set of simultaneous linear equations is inverted to get the modified sums and then the change is distributed proportional to the intensity value to the 4 pixels in each part. The parameter v is taken as 2.

If only 2 bits are embedded per block then the distortion can be reduced and a capacity of 1/8 Bits per pixel is achieved.

Table 5 Improved capacity Embedding





2 bits per 4×4 block	4 bits per 4×4 block

The error of recovery, while varying the JPEG compression quality setting the parameter v at 2 for 4 bits per block and 2 bits per block are shown in Figure 10 and 11.

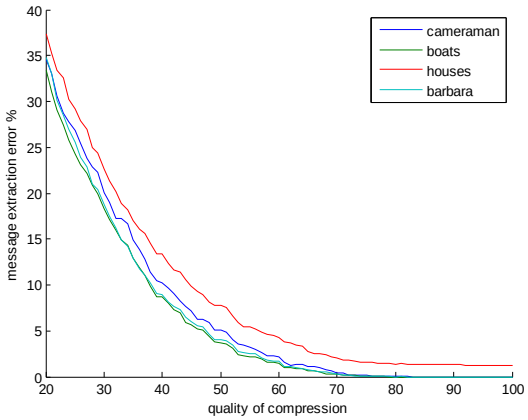


Figure 10 4 bits per block

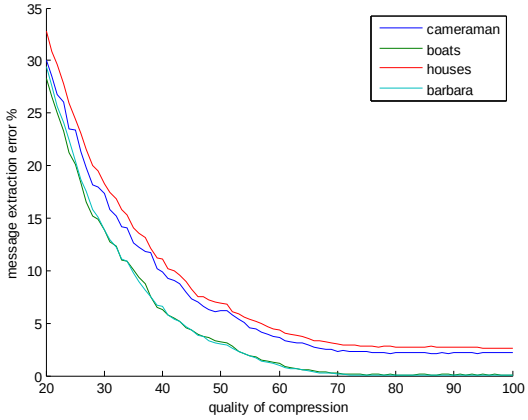


Figure 11 2 bits per block

5. CONCLUSION AND FUTURE WORK

By embedding the secret message as a modulation of mean values of image blocks it is demonstrated that steganography can be done in a way robust to stego image modification by image processing transformations such as JPEG compression, resizing and the addition of noise. Optimal values for the parameters are also shown.

The major disadvantage of the proposed method compared to the original LSB matching or the LSB matching revisited is the poor embedding capacity. The modifications proposed improve the embedding rate but may cause high distortion. By adapting the quantization parameter q and block size b according to the properties of the image region it may be possible to improve the embedding capacity without losing out on the other advantages.

6. REFERENCES

[1] Ingemar. J. Cox et al, "Digital Watermarking and Steganography,", 2nd ed. Morgan Kaufmann series in computer security.

[2] R. Chandramouli, M. Kharrazi, and N. Memon, Image steganography and steganalysis: Concepts and practice. In T. Kalker, Y. M. Ro, and I. Cox, editors, Digital Watermarking, 2nd International Workshop, IWDW 2003, Seoul, Korea, October 20–22, 2003, volume 2939 of LNCS, pages 35–49. Springer-Verlag, New York, 2004.

[3] W. Cary Huffman and Vera Pless, Fundamentals of error-correcting codes, Cambridge University Press 2003.

[4] N. F. Johnson, S. Katzenbeisser, "A Survey of steganographic techniques", in S. Katzenbeisser and F. Petitcolas (Eds.): Information Hiding, pp. 43-78. Artech House, Norwood, MA, 2000.

[5] A. Westfeld and A. Pfitzmann. Attacks on steganographic systems. In A. Pfitzmann, editor, Information Hiding, 3rd International Workshop, IH'99, Dresden, Germany, September 29–October 1, 1999, volume 1768 of LNCS, pages 61–75. Springer-Verlag,New York, 2000.

[6] Reliable Detection of LSB Steganography in Grayscale and Color Images, with M. Goljan and R. Du, Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001, pp. 27-30.

[7] S. Dumitrescu, X. Wu, and N. Memon. On steganalysis of random LSB embedding in continuous-tone images. In Proceedings ICIP, Rochester, NY, September 22–25, 2002, pages 324–339, 2002.

[8] T. Sharp, "An implementation of key-based digital signal steganography," in Proc. Information Hiding Workshop, Springer LNCS 2137, pp. 13–26, 2001.

[9] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," in Proc. SPIE Security Watermarking Multimedia Contents, vol. 5020, 2003, pp. 131–142.

[10] A. Ker, "Steganalysis of LSB matching in greyscale images," IEEE

[11] Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.

[12] Mielikainen,J, "LSB Matching Revisited", IEEE Signal Processing Letters, vol 13, Issue 5pg285-287, May 2006.