A NOVEL SPREAD SPECTRUM IMAGE STEGANOGRAPHY TECHNIQUE WITH LOW BIT ERROR RATE

A Nagalinga Rajan[1], P Eswaran[2], R Sunder [3]

[1]*Reasearch Scholar, Manonmaniam Sundaranar University, Tirunelveli, (India)*

[2]*Assistant Professor, Alagappa University, Karaikudi, (India)*

[3]*Reasearch Scholar, Manonmaniam Sundaranar University, Tirunelveli, (India)*

ABSTRACT

Spread spectrum image steganography offers high robustness as well as low detectability. The embedded images are statistically and visually indistinguishable from images corrupted by device noise and therefore it cannot be detected by steganalysis. However these methods involve approximate noise estimation algorithms and suffer from high bit error rates at the extraction stage. Hence they require the usage of high redundancy error correcting codes to compensate for the error, thereby drastically reducing the effective embedding capacity. This paper proposes a novel technique to reduce the error rates of extraction by preprocessing the cover images, hiding only a part of the discrete cosine transform coefficients of the message signal and employing a split bregman optimization based extraction stage. The split bregman method has been successfully employed in recovering random binary signal that has undergone the loss of transform coefficients. The bit error rates are reduced to an average of below 5% giving an effective payload of 0.8745 bits per pixel compared to an error rate of above 20% and 0.04 bits per pixel in existing spread spectrum image steganography method. The performance of the method and the effects of various parameters are analyzed using a database of 4000 images. The inability of standard steganalysis tools to distinguish the stego-images from noisy images is demonstrated. The proposed method offers practical and effective secret communication in combination with low redundancy error correcting codes.

Keywords: Image Steganography, Spread Spectrum, DCT, Steganalysis, Binary Signal Recovery, Split Bregman Method, Gaussian Noise, Error Correcting Codes

I INTRODUCTION

The issue of data security and privacy is increasingly becoming critical in the modern networked age. Cryptographic techniques allow communication in which the content is not exposed to anybody other than the intended recipients. But the presence of secretive communication can be easily detected by observers. This prevents many socially beneficial but controversial communication and organization of individuals like protest movements against authoritarian regimes across the world. Steganography offers an avenue for secret communication without raising suspicion in passive observers [1].

Steganographic techniques embed a hidden message into a cover medium such as images, audio, video and text. Among other cover media, images are highly desirable due to the following reasons [2]:

1. Pervasiveness of Images:

Images are present in the world wide web in enormous quantities. The number of images uploaded at any time is too high to allow scanning for secret communication.

2. Data Redundancy:

Images have high data redundancies which allow the embedding of secret bits without significantly altering the content.

3. Data Throughput:

Images are shared by everyone and therefore it raises little suspicion while allowing high secret data throughput.

Several image steganographic techniques with unique advantages and disadvantages exist in literature. The objectives of a good steganographic technique [1] are:

1. Imperceptibility:

The stego-image must remain indistinguishable from the cover image to a casual human observer.

2. Capacity:

The method must allow high embedding capacity.

3. Security:

The presence of hidden data must not be detectable by any of the steganalysis tools like statistical analysis.

Spread spectrum is the technique of modulating a narrow band signal with a wideband signal so that the energy of the resultant signal is spread evenly across a wider spectrum and therefore hard to detect [3]. Spread Spectrum Image Steganography (SSIS) typically modulates the binary message signal into a white gaussian noise signal and the result is added to an image. This resultant signal is similar to white gaussian noise. By carefully adjusting the power of the embedded signal it is possible to achieve both imperceptibility of the hidden message and reasonable recovery of the signal. The stego-images produced by SSIS will be indistinguishable from images corrupted by white gaussian noise. An error correcting code is incorporated into the embedding so that the errors in signal recovery can be corrected [4].

A brief review of various steganographic methods is presented in section 2 along with a brief review of SSIS system. The proposed method is explained in section 3. Experimental results and analysis are presented in section 4 and conclusion is offered in section 5.

II RELATED WORK

Least significant bit replacement (LSBR) is the simplest steganographic scheme. It hides the message bits in the least significant bits of the cover pixels [5]. However it can be easily detected by its asymmetrical treatment of even and odd valued pixels. Several techniques like the pair of values analysis by Westman and Pfitzmann in [6], RS Steganalysis by Fridrich et al. in [7] and primary sets technique proposed by Dumitrescu et al. in [8] can be used to

detect LSBR. LSB Matching (LSBM) is an improvement over LSBR where the least significant bit of the cover pixels are randomly increased or decreased by one to match the message bits as needed. LSBM can be detected by the center of mass (COM) of the histogram characteristic function (HCF) introduced by Harmsen et al. in [9] and more effectively by adjacency HCF COM by A D Ker in [10]. LSB Matching Revisited (LSBMR) was proposed by Mielikainen in [11]. Edge adaptive Image Steganography based on LSBMR was proposed by Weiqi Luo et al in [12]. This method can be detected by targeted steganalysis using B-Spline fitting proposed by Shunquan Tan in [13]. Higher embedding rates are achieved using Diamond encoding by Chao et al. in [14] and Adaptive pixel pair matching by Wieng Hong and Tung-Shou Chen in [15]. These methods operate in the spatial domain of the image. Several transform domain techniques are also proposed where the message bits are hidden in DCT coefficients. Some of the techniques that fall under this category are F5 [16], Outguess [17], JSteg [18] etc which work in JPEG images. Steganalysis of F5 was performed by Fridrich et al in [19]. Many of the common steganographic methods have their implementation available online [20]. All the above mentioned methods strive to preserve certain vital statistics of images to avoid detection.

SSIS was analyzed by Marvel et al. in [4] . The method combines spread spectrum communication techniques, error correcting codes (ECC) and image processing to achieve hidden communication. Optimum signature design for SSIS was proposed by Gkizeli et al. in [21]. The robustness of SSIS was improved by Youail R S et al. in [22]. Quantization techniques were used to improve SSIS by Chun Hsiang Huang et al in [23]. SSIS was adapted to the DCT domain by Agrawal et al. in [24]. Selecting cover images for SSIS using correlation coefficient was considered in [25] by Yifeng Sun. SSIS was improved further based on complete complementary codes by Mayuzumi et al. in [26]. SSIS does not aim to preserve image models or statistics but masks the stego-noise as the result of natural processing. The bit error rates however are very high (>20%), requiring the usage of high redundancy ECCs and consequently the effective data embedding rates are low. In general error in the recovery of bits is unavoidable in all blind steganography schemes. Stochastic Modulation (SM) by Fridrich and Goljan in [27] is another approach to masking embedding as natural processing that improved the capacity up to 0.8 Bits per Pixel (BPP). A description of the basic SSIS is given below.

The major components of SSIS system are:

1. Stego Noise Generation

   The message is usually encrypted with key(s) (K_1) and an ECC is applied to get the embedding signal. This signal is modulated into a white gaussian noise signal which is generated by a pseudo random generator with seed (K_2) . The resultant signal is interleaved using a third key (K_3). This process ensures that bit errors in recovery do not occur together thus enabling the ECC to perform better.
2. Stego Noise addition

   The stego noise is added to the cover image and quantized to get the stego image.
3. Image processing operation

A restoration filter is applied to the stego image during the extraction stage at the receiver side. This process utilizes the piecewise smooth nature of natural image signals and gives an estimate of the original cover image. This estimate is subtracted from the stego image to recover the stego noise.

4. Message extraction

The stego noise is de-interleaved using K_3 and demodulated by generating the same pseudorandom noise using (K_2). The ECC decoder is then applied and decryption takes place using (K_1) to get the estimate of the message. If an appropriate ECC is used, the message is recovered without any errors.

The SSIS system incurs an error rate of above 24 % warranting the use of (889,35) ECC. This severely degrades the embedding capacity to less than 0.1 BPP.

This paper proposes a cover image preprocessing, DCT domain embedding and message extraction using split Bregman iterations. The method masks the embedding as natural processing. Experimental results demonstrate that the bit error rates are reduced to below 5% on average. This allows the use of Reed Solomon ECC [28] with parameters $k=223$, $s=16$ and $n=255$ to achieve a capacity of 0.8745 BPP.

III PROPOSED METHOD

The schematic diagram for the encoder and decoder of the proposed method is shown in fig.1. The steps involved in encoding are as follows.

3.1 Cover Image Preprocessing

The cover image I_c is subjected to low pass filtering operation on a block by block basis. The image is divided into distinct blocks of size $w \times w$ and discrete cosine transform (DCT) in applied to the blocks. Then the coefficients are arranged in zigzag order of increasing frequency and the higher frequency coefficients are nullified. The fraction of coefficients to discard is a design parameter α and the last αw^2 coefficients are made equal to zero. This preprocessing step creates space for storing the stego noise while maintaining the cover image information as much as possible. Since the bulk of information in natural images are present in the lower frequencies this step retains the visual characteristic of the image. Also this step does not necessarily raise suspicion since removing high frequencies is a common image processing operation in compression [29].

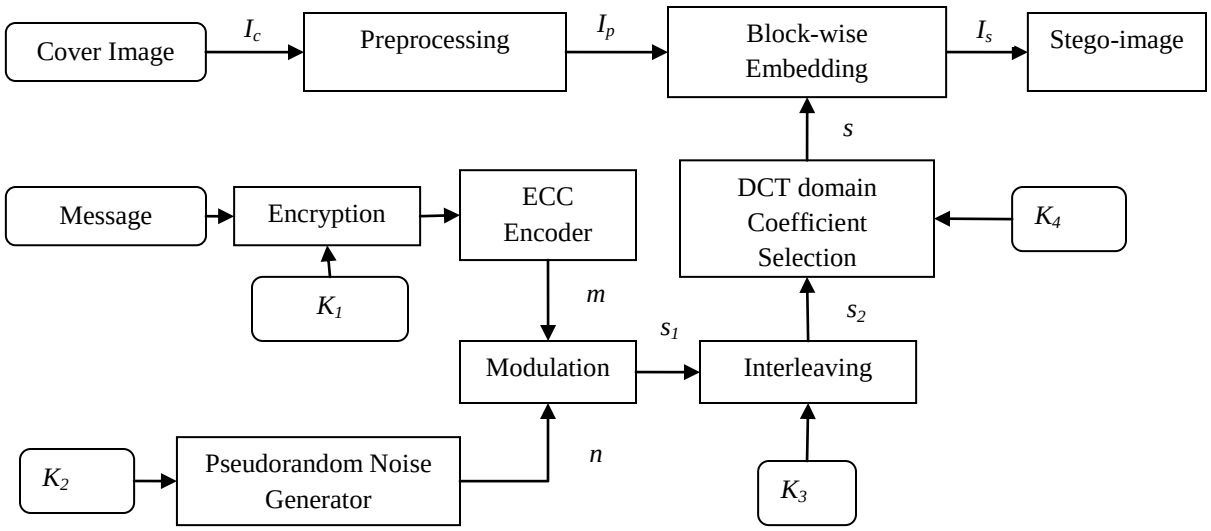

Figure1. Schematic Diagram of Encoder

3.2 Stego noise generation

The message is encrypted using a set of keys, K_1 depending on the choice of cryptosystem. Then the encrypted bits are encoded using an error correcting codes such as Reed Solomon codes which is based on oversampling a polynomial with the signal elements as coefficients [28]. A pseudo random noise generator seeded with K_2 is used to generate a normally distributed 2D noise signal n of the same size as I_c. The binary message is encrypted, ECC is applied to it and is reshaped to the same size as I_c with values {-1,1} in place of the bit values {0,1}. These two matrices are multiplied element by element to get s_1 which still has the same distribution of n. The interleaving step ensures that the bit recovery errors do not occur in bursts which will hinder the performance of the ECC [4]. Also the pseudorandom generator for the interleaving process is seeded with key K_3.

3.3 DCT Coefficient Selection

The stego noise is transformed to DCT domain in blocks of size $w \times w$ and some of the coefficients are selected to be embedded in the image. The fraction of coefficients to be selected is α corresponding to the nullified DCT coefficients of the image blocks. The parameter α is a tradeoff between distortion and message integrity. It can be selected in the range of (0.5 - 0.9) for efficient recovery of message bits while keeping distortion reasonably low. This will be explained further in section 3.5. The selection itself is pseudo randomly generated with seed K_4 and used for all the blocks. The selected coefficients are rearranged in positions corresponding to the nullified DCT coefficients of the image blocks. The Expected magnitudes of the DCT coefficients in this case are equal as confirmed by the box plot in fig. 2. Therefore any preferential selection of coefficients to be hidden is not useful.

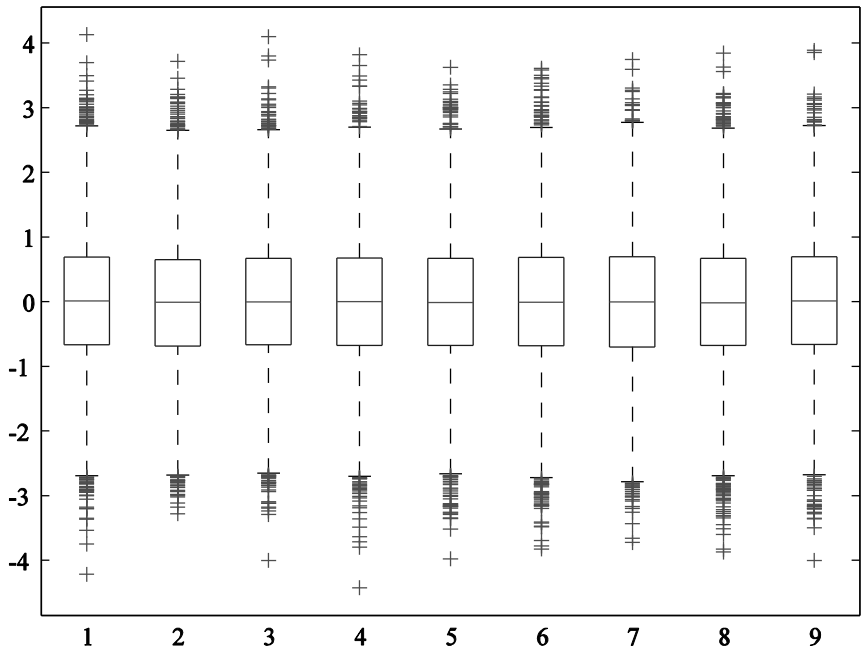

Figure 2. Box plot of DCT coefficients for b=3 over 10000 realizations

3.4 Stego Image Generation

The stego noise *s* is added to I_p block by block. A high value of embedding strength λ gives more robustness in signal recovery. The selected coefficients of stego noise *s* get preserved in the nullified locations of the blocks of I_p in the DCT domain. It can be experimentally demonstrated that *s* is sufficiently indistinguishable from gaussian noise by steganalysis.

3.5 Message Recovery

Decoding process of the proposed system does not involve image restoration. Instead Split Bregman iterations are utilized to recover the binary signal which has lost its coefficients partially in the DCT domain. The following optimization problem is solved for every block.

$$\min_u \|K(F.*N)u - b\|^2 \; s.t. \; u = \{-1,1\} \quad (1)$$

Here *b* is the vector composed of selected coefficients in DCT domain, *u* is the binary signal from the interleaving step in vector form that needs to be recovered, *N* is a matrix formed by replicating the pseudo random noise vector *n*

generated at the receiver side. The DCT operation matrix *F* is calculated as the kronecker square of column-wise DCT of identity matrix.

$$F = D \otimes D \tag{2}$$

$$D_{:,i} = dct\left(I_{:,i}\right) \tag{3}$$

F and *N* are multiplied together element by element. *K* is a rectangular matrix that selects only the known coefficients. It can be formed by removing the appropriate rows of identity matrix. Referring to *(F.*N)* as *A* and allowing *u* to vary in the range of (-1,1) , the optimization problem in equation (1) is transformed to a convex optimization problem as in equation (4). The reader is referred to Theorem 3.1 in [30] for a discussion on the equivalence of the two formulations. It is applicable to this case when α is sufficiently high.

$$\min_u \|KAu - b\|^2 \; s.t - 1 \leq u \leq 1 \tag{4}$$

The Split Bregman algorithm to solve equation (4) is adapted from []. The vector *u* is initialized by the inverse DCT of vector *b* with zeros in locations of missing coefficients referred to as *b'*.

Algorithm 1 The Split Bregman Algorithm for Solving Equation 4:

Initialize: The initial guess $u = (A)^{-1}b'$

Let $b_0 = b$

While $\|Au - b_0\|^2$ not small enough and for a maximum of i_{max} iterations do

$d \leftarrow P(u - v)$

$u \leftarrow ((A^{-1}(b^2 \lambda K^T K + I)^{-1})^{-1}A)^{-1}(\lambda(KA)^T b + P(d) + v)$

$u \leftarrow sign(u)$

$v \leftarrow v + P(d) - u$

$b \leftarrow b + b_0 - KAu$

end

Output: u

The function *P* clips the arguments in the range of [-1,1]. The convergence of the algorithm is very much dependent on the binary signal and is more likely for high value of α. The matrix inversion is performed only once for all the iterations and can be used for all the blocks. The maximum iterations i_{max} is set to 100.

$$P(d) = \begin{cases} 1, & d > 1 \\ d, & -1 \leq d \leq 1 \\ -1, & d < -1 \end{cases} \tag{5}$$

The schematic for the decoder is shown in figure 3. The received stego image is divided into blocks and the selected coefficients are rearranged in their original positions using K_4. The binary message is recovered through Algorithm 1. The extracted binary signal is de-interleaved using K_3, demodulated with the known pseudorandom noise using K_2 and decrypted using K_1 to get the hidden binary message.

Reed Solomon codes are used as error correcting codes to compensate for the errors in signal recovery. The four keys must be shared between the communicating parties beforehand. The key sharing mechanism within the steganographic setting is an open research issue . The parameters of the proposed method are the block size *w* and fraction α. The fraction α must be in the range of (0.5-1.0) and represents a tradeoff between lowering distortion and increasing the accuracy of recovery. Results show that an ideal choice of α is 0.7 which limits the recovery error below 5%.

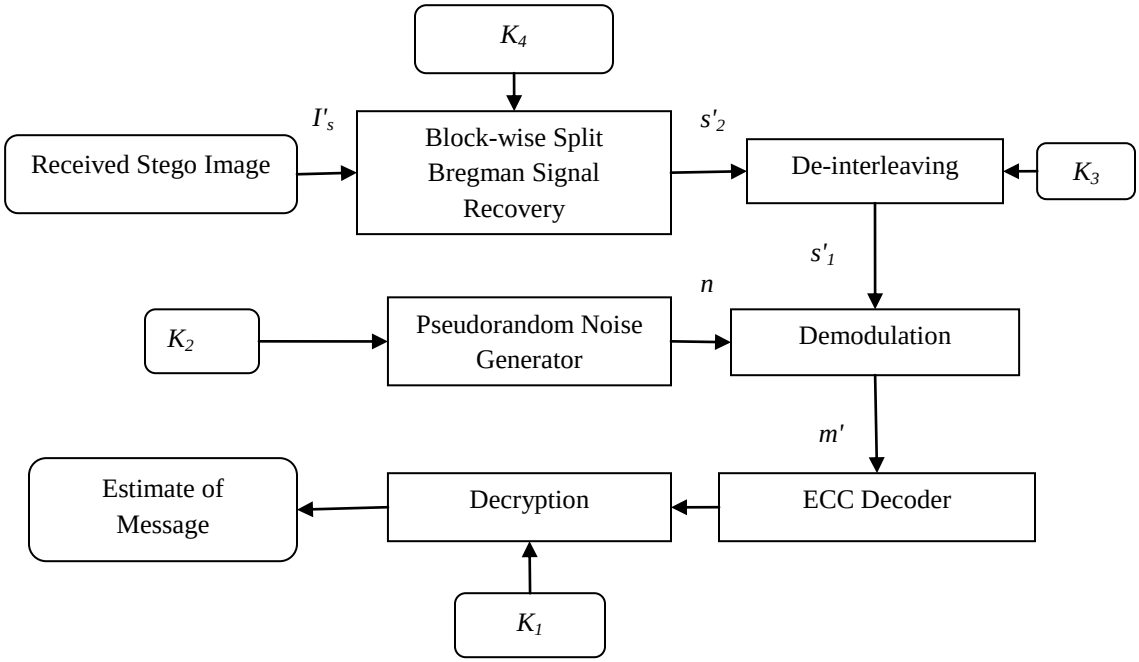

Figure 3. Schematic Diagram of Decoder

IV PERFORMANCE ANALYSIS

A large database of uncompressed images are collected from various sources such as UCID, RSP and combined with standard test images. All experiments are conducted on this image database and the measures presented are averaged over the images. Figures 4 and 5 show the results on cameraman and lena grayscale images for $\alpha = 0.7$, $\lambda = 1$ and b=8. Figure 6 shows a magnified view of lena image which shows the effect of stego noise.

The proposed method masks the embedding operation as the effect of image compression and the presence of additive white Gaussian noise and involves the preprocessing of cover images. In this context, distortion of the stego image with respect to both the raw cover (P_1) and the preprocessed cover (P_2) are measured using Peak Signal to Noise Ratio (PSNR). PSNR is defined as the ratio of the power of peak image signal to the power of noise component expressed in logarithmic scale as decibels (dB). A higher value of PSNR (greater than 30) implies that the distortion is too low to be recognized by a casual human observer. Table 1 gives the average PSNR values for various choices of *w* and α. The recovery is computationally impractical for block sizes higher than 32. The

degradation of the PSNR is seen with increasing α. Since the embedding is masked as loss of high frequencies due to compression, low values of P_1 does not imply poor performance. The measure P_2 corresponds to the embedding and is quite high.

Figure 4. cameraman stego-image

Figure 5. lena stego-image

Raw Cover Stego (λ=1) Stego (λ=10)

Figure 6. Magnified view of Stego Noise in Lena Image

Table 1. PSNR of Stego Image with Raw Cover (P_1), Preprocessed Cover (P_2) for λ = 1

w / α	4		8		16		32	
	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2
0.5	45.66	49.64	44.56	50.39	42.68	50.44	42.92	50.46
0.6	43.83	49.65	43.03	50.39	41.2	50.45	41.42	50.45
0.7	40.49	49.64	40.70	50.39	39.38	50.45	39.61	50.45
0.8	37.38	49.62	37.65	50.40	37.02	50.44	37.43	50.45
0.9	31.69	49.64	32.76	50.39	33.22	50.44	33.78	50.45

The accuracy of message recovery is measured as bit error rate (BER) defined as

$$BER = \frac{Number\ of\ Correctly\ Extracted\ Bits}{Total\ Number\ of\ Message\ Bits} \quad (6)$$

Table 2 presents the BER for various choices of α and b. The BER decreases with increasing α and falls below 5 % for α > 0.6. The standard version of SSIS [] incurs a BER of 24-27 % requiring (889,35) error correcting coder yielding embedding capacity of 0.04 BPP. The proposed method requires the use of Reed Solomon ECC with parameters *k=223, s=16* and *n=255* yielding an embedding capacity of 0.8745 BPP.

Table 2 Bit Error Rate of Message Recovery (%) for λ = 1

W / α	4	8	16	32
0.5	15.44	13.27	13.21	13.20
0.6	5.30	5.21	5.20	5.20
0.7	3.21	3.20	3.18	3.14
0.8	0.61	0.60	0.60	0.60
0.9	0.35	0.35	0.35	0.35

V SECURITY ANALYSIS

The effectiveness of the proposed method to evade detection by steganalytic methods is established in this section. T Pevny et al proposed Subtractive Pixel Adjacency Matrix (SPAM) in [31]. SPAM is a highly effective universal steganalysis method based on a feature set composed of pixel intensity value transition probabilities along eight directions. It employs a soft margin support vector machine (SVM) classifier with Gaussian kernel to classify stego-images from normal images. The MATLAB implementation of SPAM is available online at [32]. The receiver operating characteristic curves (ROC) for classification by first order SPAM of the proposed method is shown in Figure 7 for the parameter values α = 0.7 and b = 8. Figure 8 shows the ROC curves for second order SPAM. The performance measures for the classification is given in Table 3. In the experiment the SPAM classifier was tasked with classifying stego-images of the proposed method from images corrupted by additive white gaussian noise of similar intensity as the stego-noise. It can be seen that SPAM steganalysis cannot be done very effectively with accuracy below 75 % thus demonstrating the effectiveness of the proposed method.

Table 3 Performance measure for SPAM steganalysis

	Accuracy (%)	Specificity (%)	Sensitivity (%)
SPAM order = 1, 162 features	71.17	64.41	89.92
SPAM order = 2, 686 features	73.44	78.59	69.86

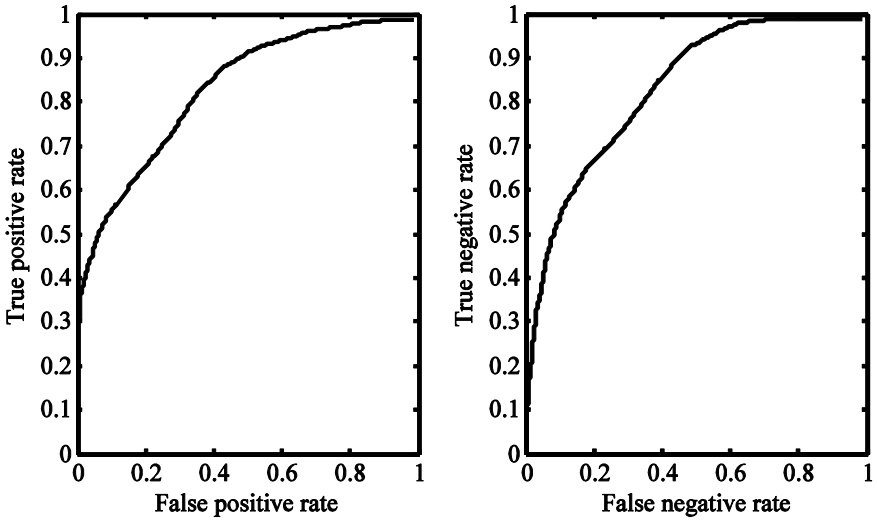

Figure 7. ROC Curves for SPAM first order (162 features)

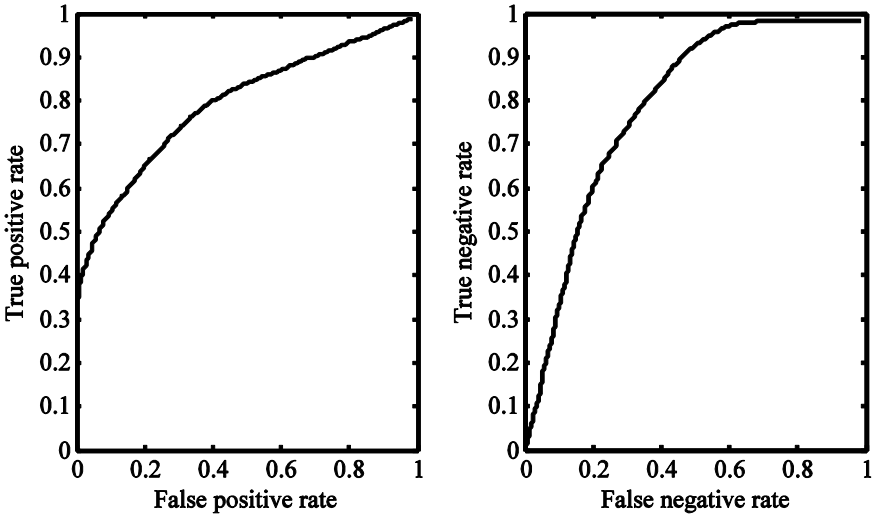

Figure 8. ROC Curves for SPAM second order (686 features)

VI CONCLUSION

This paper proposed a novel method for spread spectrum image steganography. The method hides partial transform domain coefficients in the visually least significant positions of the image spectrum. The inaccurate filtering process

for estimating the stego-noise is not necessary due to the special embedding procedure. It employs split Bregman iterations to recover the binary message with much higher accuracy than the conventional SSIS method. The error of recovery is reduced from greater than 20 % in conventional SSIS to less than 5% on average. The need for high redundancy ECC is thus removed thereby improving the effective embedding capacity from below 0.1 BPP to 0.8745 BPP. It is also shown that the steganalysis of the method by state of art steganalysis cannot be done reliably. Masking the embedding as natural processing is an effective approach to bringing steganography to real life applications. Future research effort may decrease the bit error rate further by improving the convergence of the split Bregman iterations. Also effort must be made to decrease the computational complexity of the proposed method.

REFERENCES

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

[2] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An overview of image steganography" *in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa*, June/July 2005 (Published electronically)

[3] Cox, I. J., J.Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio, and video", *Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland*, vol. 3, pages 243-246, September 1996.

[4] Lisa M. Marvel, Charles G. Boncelet, Jr., and Charles T. Retter, "Methodology of spread-spectrum image steganography", *Army Research Laboratory, ARL-TR-1698*, June 1998.

[5] C. K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition 37(3)*, pages 469-474, 2004.

[6] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems", *Information Hiding, 3rd International Workshop, IH'99, Dresden, Germany*, September 29 - October 1, 1999.

[7] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB steganography in color and grayscale images", *IEEE Multimedia*, vol. 8, pages 22-28, 2001.

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

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

[10] A. D. Ker, "Steganalysis of LSB matching in grayscale images", *IEEE Signal Processing Letters*, vol. 12, no 6, pages 441-444, June 2005.

[11] J. Mielikainen, "LSB Matching Revisited", *IEEE Signal Processing Letters*, Vol. 13, Issue 5, pages 285-287, May 2006.

[12] W. Luo , F. Huang and J. Huang, "Edge adaptive image steganography based on LSB matching revisited", *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pages 201 -214 2010.

[13] Shunquan Tan and Bin Li, "Targeted steganalysis of edge adaptive image steganography Based on LSB Matching Revisited Using B-Spline Fitting", *IEEE Signal Processing Letters*, Vol. 19, Issue 6, pages 336-339, April 2012.

[14] R. M. Chao, H. C. Wu, C. C. Lee and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP Journal of Information Security*, vol. 2009, 2009.

[15] W. Hong and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching", *IEEE Transactions on Information Forensics and Security"*, vol. 7, No. 1, February 2012.

[16] Andreas Westfeld, The Steganographic Algorithm F5, 1999, Online at http://wwwrn.inf.tu-dresden.de/˜westfeld/f5.html

[17] OutGuess, Steganography Detection with Stegdetect [Online]. (December 29, 2003). Online at http://www.outguess.org/detection.php

[18] Derek Upham, Jpeg-Jsteg-V4, Online at http://www.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz

[19] J. Fridrich, M. Goljan and D. Hogea, "Steganalysis of JPEG Images: Breaking the F5, in *Petitcolas, F.A.P. (ed.) Information Hiding 2002. LNCS*, vol. 2578, pages 310–323. Springer, Heidelberg 2003.

[20] [Hide and Seek]: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/cypherpunks/steganography/hdsk41b.zip

[S-Tools]: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip

[Stella] : http://wwwicg.informatik.uni-rostock.de/~sanction/stella/

[Hide in Picture]: http://sourceforge.net/projects/hide-in-picture/

[Revelation]: http://revelation.atspace.biz/

[Camouflage]: http://camouflage.unfiction.com/

[JpegX]: http://www.freewarefiles.com/Jpegx_program_19392.html

[Data Stash]: http://www.skyjuicesoftware.com/software/ds_info.html

[Other Tools]: http://www.jjtc.com/Security/stegtools.htm

[F5]: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html

[OutGuess]: http://www.outguess.org/

[21] M. Gkizeli, D. A. Pados, M. J. Medley, "Optimal Signature Design for Spread-Spectrum Steganography," *IEEE Transactions on Image Processing*, Vol. 16, Issue 2, pages 391-405, 2007.

[22] R. S. Youail, A. Khadhim, V.W. Samawi, "Improved stegosystem using DFT with combined error correction and spread spectrum," *Industrial Electronics and Applications, 2nd IEEE Conference on ICEA*, pages 1832-1836, 2007.

[23] Chun-Hsiang Huang, Shang-Chih Chuang, Ja-Ling Wu, "Digital-Invisible-Ink data hiding based on spread spectrum and quantization techniques", *IEEE Transactions on Multimedia*, vol. 10 issue. 4, pages 557-569, 2008.

[24] N. Agrawal A. Gupta, "DCT domain message embedding in spread-spectrum steganography system", *Data Compression Conference*, page 433, 2009.

[25] Yifeng Sun and Fenlin Liu, "Selecting cover for image steganography by correlation coefficient," *Second International Workshop on Education Technology and Computer Science*, Vol. 2 , pages 159-162, 2010.

[26] R. Mayuzumi and T. Kojima, "An improvement of steganography scheme based on complete complementary codes", *International Symposium on Information Theory and its Applications (ISITA)*, pages 638-642, 2012

[27] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", *Proceedings SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents*, V Santa Clara, California, pages 191-202, 2003.

[28] S. Reed and G. Solomon, "Polynomial codes over certain finite fields", *Journal of the Society for Industrial and Applied Mathematics (SIAM)*, pages 300-304, 1960.

[29] W. B. Pennebaker and J. L. Mitchell, "JPEG still image data compression standard", *Springer 3rd Edn* , page 291, 1993.

[30] Y. Mao, "Reconstruction of binary functions and shapes from incomplete frequency information," *IEEE Transactions on Information Theory*, Vol. 58, Issue 6, pages 3642-3653, March 2012.

[31] T. Pevny, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix", *IEEE Transaction on Information Forensics and Security*, Vol. 5, Issue 2, March 2010.