A Content-adaptive Image Steganography based on SDCS

Fei Peng, Xiaolong Li and Bin Yang
Institute of Computer Science and Technology, Peking University, Beijing 100871
E-mail: {pengfei,lixiaolong,yangbin}@icst.pku.edu.cn

***Abstract*—The "sum and difference covering set" (SDCS) is a steganographic technique which provides high embedding efficiency. In this paper, we implement SDCS in image steganography by searching an appropriate SDCS for high embedding efficiency and low complexity. Thus the contamination in smooth areas of image is evident for steganalyzer, we propose a novel content-adaptive steganographic scheme based on SDCS, in which the hidden data are embedded in noisy areas of cover image evaluated by a "noise level" sorting. The experimental results show that our scheme enhance the steganographic security compared with some state-of-the-art works, and the high visual quality of stego image is preserved with considerable embedding rate.**

I. Introduction

Steganography is a technique of covert communication, whose goal is to embed secret message into cover data (e.g., digital images) in such a way that the stego data cannot be discerned except for the intended recipients. As the contrary technique of steganography, steganalysis aims to detect the existence of secret message. The image steganalysis schemes are generally classified into the targeted ones and the blind ones: the former aim to determine whether the stego image is embedded by a specific steganographic scheme, while the latter attempt to detect the presence of data hiding regardless of the embedding method. Due to the development of steganalysis, the steganographic schemes continue improving to preserve the security against detection.

Several approaches are concerned to improve the security in steganography. Many schemes attempt to reduce the modification of the cover in embedding procedure, therefore the visual quality of stego image is similar to that of the cover. Least significant bit (LSB) replacement is a scheme of this case in the early stage [1]. In LSB replacement, the LSB of pixel is modified to match the hidden data bit, so that the modification of each pixel is at most 1. However, the steganalysis based on histogram statistics shows that LSB replacement is insecure owing to its histogram equalization. As a generalization of LSB replacement, matrix embedding pay more attention to reducing the embedding changes [2]–[5]. In matrix embedding, the embedding efficiency is concerned as an important performance evaluation, which is defined as the expected number of embedded secret data bits per pixel modification in the cover. The high visual quality is preserved in matrix embedding with considerable embedding rate.

To defend the detection of statistics, a further approach puts emphasis on keeping the statistic invariant. LSB matching (also known as ±1 embedding), for example, is an improvement of LSB replacement in which the pixel value is randomly increased or decreased by 1 if its LSB is different from the hidden data bit [6]. The extracting procedure of LSB matching reads hidden data from LSBs of pixels, with low complexity in common with LSB replacement. It is investigated that LSB matching is equivalent to a convolution of the cover, which is more secure than LSB replacement in statistical property. Many novel steganalysis schemes attempt to attack LSB matching based on histogram local extrema [7]–[9], compression technique [10]–[12], statistical moments [13], [14], center of mass of the histogram characteristic function (HCF-COM) [15]–[19], etc. In addition, some blind steganalyzers are also effective against LSB matching [20]–[23].

Recently, the steganography technique based on the sum and difference covering set (SDCS) proposed in [24], [25] popularizes LSB matching and matrix embedding to achieve both high embedding efficiency and security. In SDCS, matrix embedding is extended into finite cyclic Abel group. The embedding efficiency of SDCS is higher than matrix embedding, and the upper bound of embedding rate is also larger. Based on SDCS, Li *et al.* proposed a generalized LSB matching (G-LSB-M) scheme [25], which further improved embedding efficiency while keeping statistics resemblant. Nevertheless, G-LSB-M is simply more secure than LSB matching, and the scheme with more security is required in application.

Besides improving embedding efficiency, adaptively selecting the embedding location based on image content is an alternate approach to make the hidden data more undetectable. The main idea of content-adaptive steganography is that it is more secure to modify pixel in "noisy" regions rather than "smooth" regions by the same amount. Pixel-value differencing (PVD) [26] is an early content-adaptive steganography, which attempts to embed more data in noise regions. Some other content-adaptive noise region embedding schemes are also proposed recently [27], [28], in which the modified pixels are selected where the modification is difficult to detect. The edge-adaptive steganography [29] proposed by Luo *et al.* is a improvement of LSB matching revisited (LSB-MR) [30], in which the data are embedded into the edges in image content. This scheme can enhance security against staganalysis while keeping high visual quality of the stego image.

In noise region embedding procedure, locating noisy pixel area and embedding hidden data are relatively independent. Inspired by the high embedding efficiency of SDCS and the high security of noise region embedding, we propose a novel content-adaptive steganography in this paper, which integrates the minimization of modification, statistics resemblance and adaptive pixel selection. A novel content-adaptive noise region locating scheme is applied, in which the embedding pixels of image are sorted by their "noise level" calculated from extrema of neighbor reference pixels according to a shared key. Afterwards, an optimal SDCS is applied to embed data into the pixels with highest noise level with low complexity in application. The intended recipient is able to sort pixels by noise level from the key, and extract hidden data by SDCS. The embedding efficiency is high in our scheme with considerable embedding rate. Furthermore, the modification in noise regions of images preserves high visual quality of the stego and is difficult to detect. The experimental results show that our method is more secure than some state-of-the-art works against blind steganalysis, such as LSB matching and G-LSB-M.

The rest of the paper is organized as follows. In Section II, we introduce SDCS briefly and propose a low-complexity (6,64)-SDCS embedding scheme. The novel content-adaptive noise region embedding technique is proposed in Section III. In Section IV, we compare our steganographic scheme with other state-of-the-art schemes against blind steganalyzer. Finally, our conclusion is drawn in Section V.

II. INTRODUCTION OF SDCS

The SDCS-based steganography proposed by Li *et al.* in [24] is briefly introduced in this section. For the application of ±1 embedding, the notations denoted here are a little different from those in [24].

We denote G_M as a finite cyclic group with order M. It is proved that any M-ordered finite cyclic group is an Abel group and is isomorphic from the group $\mathbb{Z}/M\mathbb{Z}$, and we simply consider the group $\mathbb{Z}_M = \mathbb{Z}/M\mathbb{Z} = \{0, 1, ..., M-1\}$. In this case, the set

$$\mathbf{A} = \{a_1, a_2, ..., a_N\}, \quad a_i \in \mathbb{Z}_M,\ i = 1, 2, ..., N$$

is defined as a (N,M)-SDCS, if for each $m \in \mathbb{Z}_M$, there exists

$$\mathbf{S} = \{s_1, s_2, ..., s_N\}, \quad s_i \in \{0, \pm 1\},\ i = 1, 2, ..., N$$

such that $\sum_{i=1}^{N} s_i a_i = m$.

Based on the definition of SDCS, we denote some notations in (N,M)-SDCS-based steganography with the set $\mathbf{A}$. Let

$$C_m(\mathbf{A}) = \{(s_1, s_2, ..., s_N) : s_i \in \{0, \pm 1\}, \sum_{i=1}^{N} s_i a_i = m\},$$

$$|C_m(\mathbf{A})| = \inf\{\sum_{i=1}^{N} |s_i| : (s_1, s_2, ..., s_N) \in C_m(\mathbf{A})\},$$

$$D_m(\mathbf{A}) = \{(s_1, s_2, ..., s_N) \in C_m(\mathbf{A}) : \sum_{i=1}^{N} |s_i| = |C_m(\mathbf{A})|\}.$$

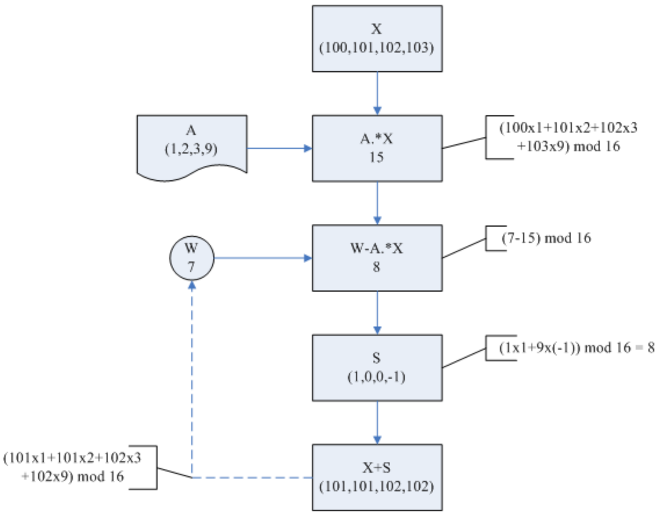


Fig. 1. An example of (4,16)-SDCS embedding and extracting.

As $\mathbf{A}$ is a SDCS, $C_m(\mathbf{A})$ and $D_m(\mathbf{A})$ are non-empty sets for each $m \in G_M$. Therefore, we define SDCS embedding function f_{emb} and extracting function f_{ext} for any embedding data $w \in \mathbb{Z}_M$: to the cover sequence $\mathbf{X} = \{x_1, x_2, ..., x_N\}, x_i \in \mathbb{Z}$ and the stego sequence $\mathbf{Y} = \{y_1, y_2, ..., y_N\}, y_i \in \mathbb{Z}$,

$$f_{emb}(\mathbf{X}, w) = \{\mathbf{X} + \mathbf{S} : \mathbf{S} = (s_1, s_2, ..., s_N) \in D_{w - \sum_{i=1}^{N} x_i a_i}(\mathbf{A})\},$$

$$f_{ext}(\mathbf{Y}) = \sum_{i=1}^{N} y_i a_i.$$

The correctness of SDCS embedding is guaranteed as follow:

$$f_{ext}(\mathbf{Y}) = \sum_{i=1}^{N} y_i a_i = \sum_{i=1}^{N} (x_i + s_i) a_i = (\sum_{i=1}^{N} x_i a_i) + (\sum_{i=1}^{N} s_i a_i)$$
$$= (\sum_{i=1}^{N} x_i a_i) + (w - \sum_{i=1}^{N} x_i a_i) = w.$$

In addition, since $\mathbf{S} \in C_m(\mathbf{A})$,

$$\|\mathbf{Y} - \mathbf{X}\|_{l^\infty} = \|\mathbf{S}\|_{l^\infty} \leq 1$$

which shows that the modification of pixel in SDCS is at most 1, thus the visual similarity between the cover and the stego is guaranteed.

Fig. 1 shows an example of embedding payload "$7 \in \mathbb{Z}_{16}$" into cover sequence (100,101,102,103) and extracting it from stego sequence (101,101,102,102), with a SDCS of (1,2,3,9) in $\mathbb{Z}_{16}$.

The embedding efficiency of (N,M)-SDCS is determined by the expected average modification per pixel under all possible embedded data, measured by the average of $|C_m(\mathbf{A})|$ for all $m \in \mathbb{Z}_M$. Obviously, the selection of $\mathbf{A}$ exerts a profound influence on the improvement of embedding efficiency. In [24], Li *et al.* prove that larger M brings higher embedding efficiency. As the embedding rate is $\frac{\log_2 M}{N}$, N will increase accompanied by M for fixed embedding rate. However, the expansion of SDCS leading to a fast increase in time complexity of SDCS construction, hence a trade-off should be made to get high embedding efficiency with acceptable complexity. In practical, we are able to traversal the SDCS with $N = 6$ in a few minutes, while several hours are required when $N = 7$. Therefore, we choose SDCS with $N = 6$ and $M = 64$ for embedding rate of 1.0 bpp, which is suitable for common application. After the traversal of (6,64)-SDCS, we select the optimal SDCS $\mathbf{A} = \{1, 2, 4, 12, 21, 28\}$ which provides minimal average modification of pixel: for any $m \in \mathbb{Z}_{64}$,$|C_m(\mathbf{A})| \leq 2$ except $|C_{18}(\mathbf{A})| = |C_{46}(\mathbf{A})| = 3$. The expected average modification per pixel of this SDCS is $(12 + 49 \times 2 + 2 \times 3)/6/64 = 0.302$, which is lower than 0.375 in edge-adaptive steganography [29]. This implies that our SDCS provides higher embedding efficiency than [29], i.e. our scheme embeds more data with the same modification of cover image.

The sequence in (6,64)-SDCS will be applied in our steganography scheme with at most 1.0 bpp embedding rate. It is worth notice that not all pixels will be selected for modification when appointed embedding rate is less than 1.0 bpp in practical. In this light, embedding pixels should be adaptively chosen based on the image content to make the modification difficult to observe.

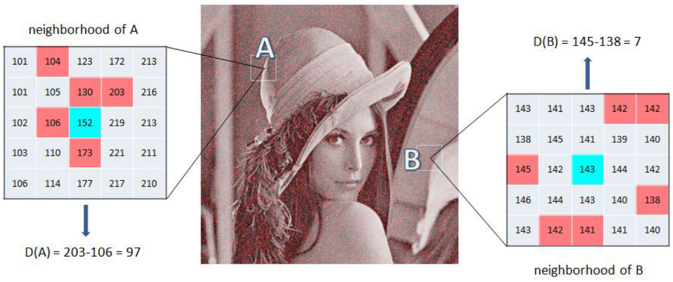
III. Content-adaptive Image Steganography

Many related works mention that the human vision is more sensitive to the modification in smooth regions rather than in noisy regions, in spite that the Peak Signal to Noise Ratio (PSNR) of the modifications in different regions are identical. In general, the characteristics of noise regions are more complicated, and they can tolerate more modification with small alteration of visual or statistical features. This concept is called “noise region embedding” and many works have attempted to investigate algorithms to locate noise region accurately for higher security. Recently, random key technique has developed in steganography to increase randomness. We propose a novel noise region embedding based on random key technique, which achieves high accuracy and low complexity in locating pixels in noise regions.

As there exists inner correlation among adjacent pixels, it is reasonable to determine the “noise level” of a pixel from its neighborhood. A pixel is predicted in noise region when the values of its neighbor pixels are significantly different. On this basis, we propose a scheme of the pixel noise level calculation based on local extrema of its neighborhood. For convenience, we regard image $\mathbf{I}$ with n pixels as a sequence $\mathbf{I} = \{I_1, I_2, ..., I_n\}$. A random key K is used in this scheme and is shared by both sender and recipient.

Noise level calculation procedure:

- Input: cover image $\mathbf{I} = \{I_1, I_2, ..., I_n\}$, random key $\mathbf{K}$.
- Algorithm:
  1) Select $\mathbf{I}^r = \{I^r_1, I^r_2, ..., I^r_m\} \subset \mathbf{I}$ as reference pixel set according to $\mathbf{K}$. Let $m = \lfloor \frac{n}{4} \rfloor$ for both sufficient embedding rate and reference accuracy. Denote $\mathbf{I}^e = \mathbf{I} - \mathbf{I}^r$ as embedding pixel set.
  2) for each pixel $i \in \mathbf{I}^e$, denote its local reference pixel value set $S_r(i)$:
     - Let $S_r(i) = \emptyset$.



101	104	123	172	213
101	105	130	203	216
102	106	152	219	213
103	110	173	221	211
106	114	177	217	210

143	141	143	142	142
138	145	141	139	140
145	142	143	144	142
146	144	143	140	138
143	142	141	141	140

Fig. 2. The example of noise level calculation in Lena.

     - Add the values of pixels which are located in 3×3 area centered at i and belong to $\mathbf{I}^r$ into $S_r(i)$.
     - If $\sharp S_r(i) < 2$, add the values of pixels which are located in 5×5 area centered at i and belong to $\mathbf{I}^r$ into $S_r(i)$.
     - If $\sharp S_r(i) < 2$, add the values of pixels which are located in 7×7 area centered at i and belong to $\mathbf{I}^r$ into $S_r(i)$.

     The symbol $\sharp$ denotes the number of different elements in the set.
  3) Calculate the noise level $D(i)$ of pixel i:

$$D(i) = \begin{cases} \max\limits_{j \in S_r(i)} j - \min\limits_{j \in S_r(i)} j, & if |S_r(i)| \geq 2; \\ -1, \quad if |S_r(i)| < 2. \end{cases}$$

     It implies that the noise level of pixel is not able to be predicted when $D(i) = -1$, and this pixel will not be used for embedding.
- Output:
  The noise level of pixels in embedding pixel set $D(\mathbf{I}^e)$.

For each pixel in embedding pixel set $\mathbf{I}^e$, higher noise level signifies higher possibility to be located in noise region. Meanwhile, the pixel values of reference pixel set $\mathbf{I}^r$ are unchanged, which indicates that the sender and the recipient are able to calculate same noise level of the pixels in $\mathbf{I}^e$ based on the shared random key, thus the correctness of the scheme is assured.

Fig. 2 gives an example of calculating noise level of pixels A and B which are centers of the two selected areas. The pixels in reference pixel set $\mathbf{I}^r$ are marked in red. We observe that A is on the edge of texture while B is on smooth area, thus the neighborhood of A is more ”complex” than the neighborhood of B. Calculation result shows that the noise level of A is higher than that of B. In embedding procedure, pixel A will be selected to embed hidden data earlier than pixel B.

Fig. 3 shows the image Lena and the pixels selected by our scheme with 10% highest noise level in $\mathbf{I}^e$, which are marked in white. It is shown that the pixels in noise region are accurately searched out by our scheme.

Based on our noise level calculation procedure above and the optimal (6,64)-SDCS proposed in Section II, we propose a content-adaptive image steganography scheme based on

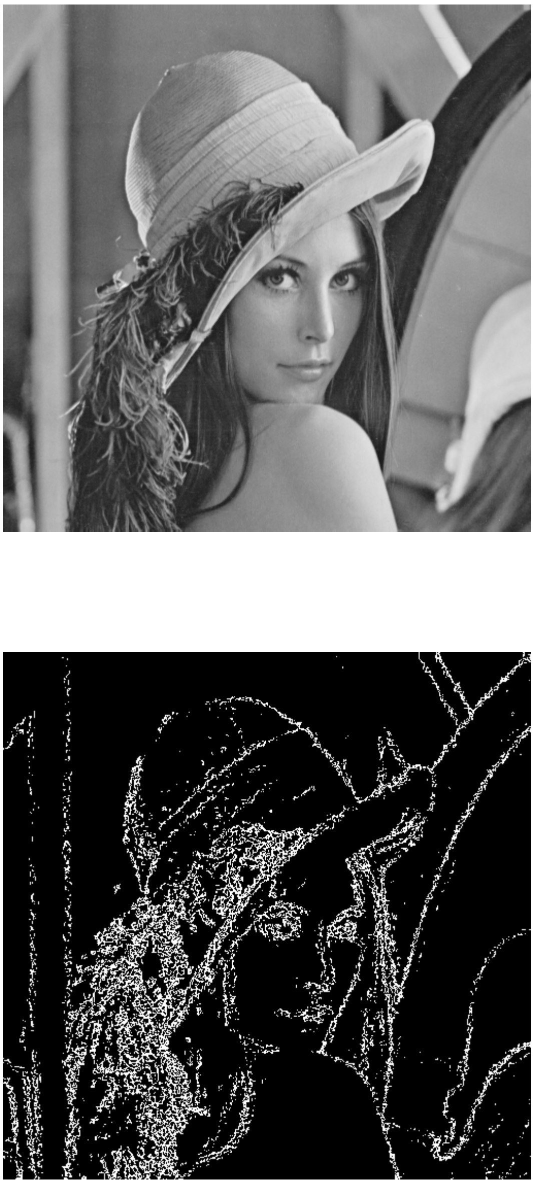


Fig. 3. The 10% pixels selected by noise level scheme in Lena.

noise region embedding and SDCS. The side information in embedding application is that the sender should inform the recipient of the ending position of embedding scheme. As the embedding rate of (6,64)-SDCS is 1.0 bpp for each embedding pixel sequence, we calculate the practically embedded data length with side information of ending position

$$len = \log_2 n + |\mathbf{W}| \tag{1}$$

where $|\mathbf{W}|$ is the length of data in binary and n is the size of image, which are both decided before embedding. Therefore, we can embed len with $\log_2 n$ bits first as the side information, and then embed $\mathbf{W}$. The recipient will recognize that the first $\log_2 n$ bits of extracted binary data are side information, and execute extracting according to the ending position.

Embedding Procedure:

- Input: cover image $\mathbf{I} = \{I_1, I_2, ..., I_n\}$, random key $\mathbf{K}$, binary embedding data $\mathbf{W}$.
- Algorithm:
  1) calculate embedding length len by Eq. (1) and use $\log_2 n$ bits to record len before $\mathbf{W}$, getting new payload $\mathbf{W}'$.
  2) Select reference pixel set $\mathbf{I}^r = \{I^r_1, I^r_2, ..., I^r_{\lfloor \frac{n}{4} \rfloor}\}$ according to $\mathbf{K}$. Get embedding pixel set $\mathbf{I}^e = \mathbf{I} - \mathbf{I}^r$.
  3) For each pixel $i \in \mathbf{I}^e$, calculate its noise level $D(i)$ as described in **Noise level calculation procedure**.
  4) Sort the pixels in I^e into $I^e_1, I^e_2, ..., I^e_{\lceil \frac{3n}{4} \rceil}$ with descending order of their noise level.
  5) According to the sorting, segment sorted I^e into cover sequences with 6 pixels in each sequence.
  6) Embed $\mathbf{W}'$ into cover sequences using (6,64)-SDCS until all data are embedded. Each sequence embeds 6 bits of binary payload which is regarded as an element of $\mathbb{Z}_{64}$.
- Output: stego image $\mathbf{J}$.

The extracting procedure for recipient is convenient. The recipient will extract len from first $\log_2 n$ of binary payload bits and then carry out extracting according to this side information.

Extracting Procedure:

- Input: stego image $\mathbf{J} = \{J_1, J_2, ..., J_n\}$, random key $\mathbf{K}$.
- Algorithm:
  1) Select reference pixel set $\mathbf{J}^r = \{J^r_1, J^r_2, ..., J^r_{\lfloor \frac{n}{4} \rfloor}\}$ according to $\mathbf{K}$. Get embedding pixel set $\mathbf{J}^e = \mathbf{J} - \mathbf{J}^r$.
  2) For each pixel $j \in \mathbf{J}^e$, calculate its noise level $D(j)$ as described in **Noise level calculation procedure**.
  3) Sort the pixels in J^e into $J^e_1, J^e_2, ..., J^e_{\lceil \frac{3n}{4} \rceil}$ with descending order of their noise level.
  4) According to the sorting, segment sorted J^e into stego sequences with 6 pixels in each sequence.
  5) Extract $\mathbf{W}'$ from stego sequences using (6,64)-SDCS. An element of $\mathbb{Z}_{64}$ is extracted from each sequence and transformed into 6 bits in binary.
  6) When first $\log_2 n$ bits are extracted, read len from them and get ending position. Continue extracting $\mathbf{W}'$ until reaching the ending position.
  7) Remove side information len from head of $\mathbf{W}'$ to get embedded data $\mathbf{W}$.
- Output: Binary embedded data $\mathbf{W}$.

As the reference pixel set $\mathbf{I}^r$ are same towards sender and recipient due to the shared key, the recipient is able to sort embedding pixel set $\mathbf{I}^e$ with the same order by the sender, and the reversibility of SDCS guarantees the correctness of our steganography scheme.

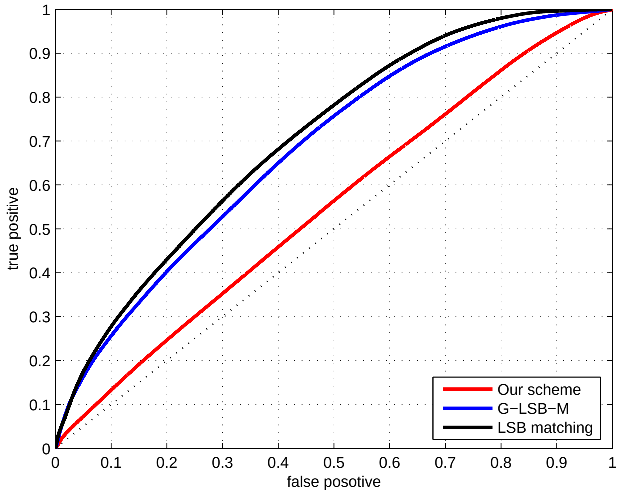


Fig. 4. The ROC curve of WAM steganalyzer.

The time complexity of our steganography scheme is fairly low. In preprocessing, the sender and recipient can calculate $D_m(\mathbf{A})$ for all m according to $\mathbf{A}$. For each image, the noise level of embedding pixel set $\mathbf{I}^e$ is calculated, and ±1 to pixels of $\mathbf{I}^e$ is applied according to data and m. The steganography scheme is applicable to large-scale image set for mass data embedding.

IV. Experimental Results

Our novel steganography scheme is compared with LSB matching [6] and its improvement G-LSB-M [25]. We use NRCS image set for our experiment, which contains 3,000 images in bitmap format. In pretreatment, the images are transformed into gray-level images, cropped to square and downsampled to the size 512×512. Afterwards, the cover images are respectively embedded by three embedding schemes with embedding rate of 0.5 bpp.

Since no targeted steganalyzer is proposed against SDCS, we apply wavelet absolute moment (WAM) steganalyzer [20], which is a high-accuracy blind steganalyzer against various of steganography schemes. The 4-folded cross-validation is applied in our experiment, in which 25% of the WAM features are used for training by Fisher linear discriminant (FLD) classifier and the rest 75% are used for testing. We test 4 times in each validation circulation, and the cross-validation is repeatedly applied for 100 times. The average receiver operating characteristic curves (ROC) of all tests are shown in Fig. 4.

The area under ROC curve (AUC) measures the general probability of correct classification between cover and stego image. The steganalyzer is effective in detection when AUC is close to 1, while it fails when AUC is near 0.5 which indicates random guessing. In Fig. 4, the AUC of our scheme is 0.550, while the AUCs of LSB matching and G-LSB-M are 0.706 and 0.684 respectively. The experimental result implies that our embedding scheme is generally more difficult to detect than LSB matching and G-LSB-M. In application, the embedding rate may be lower, and our scheme preserves more security in this case.

V. Conclusion

In this paper, a novel content-adaptive embedding method based on SDCS and noise region embedding is proposed. First, we propose an optimal (6,64)-SDCS for high embedding efficiency in steganography with suitable complexity. Afterwards, a noise level calculation procedure is proposed to embed data in noise region to improve security, and the steganographic scheme based on SDCS and noise level calculation procedure is proposed. The experimental results show that our scheme achieves high embedding efficiency and security. In future, we will investigate the construction of optimal SDCS for higher embedding efficiency with acceptable complexity. In addition, improving the performance of noise region embedding for more security is another interesting work.

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding - A survey,” *Proc. of the IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[2] A. Westfeld, “F5 - A steganographic algorithm,” in *Proc. 4th Int. Workshop on Information Hiding*, 2001, vol. 2137 of *Springer LNCS*, pp. 289–302.

[3] J. Fridrich, P. Lisoněk, and D. Soukal, “On steganographic embedding efficiency,” in *Proc. 8th Int. Workshop on Information Hiding*, 2006, vol. 4437 of *Springer LNCS*, pp. 282–296.

[4] W. Zhang, X. Zhang, and S. Wang, “A double layered “plus-minus” one data embedding scheme,” *IEEE Signal Process. Lett.*, vol. 14, no. 11, pp. 848–851, Nov. 2007.

[5] J. Bierbrauer and J. Fridrich, “Constructing good covering codes for applications in steganography,” in *Trans. on Data Hiding and Multimedia Security III*, 2008, vol. 4920 of *Springer LNCS*, pp. 1–22.

[6] T. Sharp, “An implementation of key-based digital signal steganography,” in *Proc. 4th Int. Workshop on Information Hiding*, 2001, vol. 2137 of *Springer LNCS*, pp. 13–26.

[7] J. Zhang, I. J. Cox, and G. Doërr, “Steganalysis for LSB matching in images with high-frequency noise,” in *Proc. IEEE MMSP*, 2007, pp. 385–388.

[8] G. Cancelli, G. Doërr, I. J. Cox, and M. Barni, “Detection of +-1 LSB steganography based on the amplitude of histogram local extrema,” in *Proc. IEEE ICIP*, 2008, pp. 1288–1291.

[9] Y. Gao, X. Li, B. Yang, and Y. Lu, “Detecting LSB matching by characterizing the amplitude of histogram,” in *Proc. IEEE ICASSP*, 2009, pp. 1505–1508.

[10] C. Boncelet and L. Marvel, “Steganalysis of +-1 embedding using lossless image compression,” in *Proc. IEEE ICIP*, 2007, vol. 2, pp. 149–152.

[11] C. Boncelet, L. Marvel, and B. Henz, “Rate insensitive steganalysis of +-1 embedding in images,” in *Proc. IEEE ICIP*, 2008, pp. 1272–1275.

[12] J. Dong and T. Tan, “Blind image steganalysis based on run length histogram analysis,” in *Proc. IEEE ICIP*, 2008, pp. 2064–2067.

[13] G. Xuan, Y. Q. Shi, J. Gao, D. Zou, C. Yang, Z. Zhang, P. Chai, C. Chen, and W. Chen, “Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions,” in *Proc. of the 7th International Workshop on Information Hiding*, 2005, vol. 3727 of *LNCS*, pp. 262–277.

[14] J. Zhang and D. Zhang, “Detection of LSB matching steganography in decompressed images,” *IEEE Signal Process. Lett.*, vol. 17, no. 2, pp. 141–144, Feb. 2010.

[15] J. J. Harmsen and W. A. Pearlman, “Steganalysis of additive noise modelable information hiding,” in *Security and Watermarking of Multimedia Contents V*, 2003, vol. 5020 of *SPIE*, pp. 131–142.

[16] A. D. Ker, “Steganalysis of LSB matching in grayscale images,” *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[17] X. Li, T. Zeng, and B. Yang, “A further study on steganalysis of LSB matching by calibration,” in *Proc. IEEE ICIP*, 2008, pp. 2072–2075.

[18] X. Li, T. Zeng, and B. Yang, “Detecting LSB matching by applying calibration technique for difference image,” in *Proc. of the 10th Workshop on Multimedia & Security*, 2008, pp. 133–138.

[19] E. Zheng, X. Ping, T. Zhang, and G. Xiong, “Steganalysis of LSB matching based on local variance histogram,” in *Proc. IEEE ICIP*, 2010, pp. 1005–1008.

[20] M. Goljan, J. Fridrich, and T. Holotyak, “New blind steganalysis and its implications,” in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, 2006, vol. 6072 of *SPIE*, pp. 1–13.

[21] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” *IEEE Trans. Inf. Forens. Security*, vol. 1, no. 1, pp. 111–119, Mar. 2006.

[22] H. Gou, A. Swaminathan, and M. Wu, “Noise features for image tampering detection and steganalysis,” in *Proc. IEEE ICIP*, 2007, pp. 97–100.

[23] B. Li, J. Huang, and Y. Q. Shi, “Textural features based universal steganalysis,” in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 2008, vol. 6819 of *Proc. SPIE*, pp. 681912–681912–12.

[24] X. Li, T. Zeng, and B. Yang, “Improvement of the embedding efficiency of LSB matching by sum and difference covering set,” in *Proc. IEEE ICME*, 2008, pp. 209–212.

[25] X. Li, B.Yang, D. Cheng, and T. Zeng, “A generalization of LSB matching,” *IEEE Signal Process. Lett.*, vol. 16, no. 2, pp. 69–72, Feb. 2009.

[26] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, Jun. 2003.

[27] J. Fridrich, M. Goljan, P. Lisoněk, and D. Soukal, “Writing on wet paper,” *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3923–3935, October 2005.

[28] Y. Lu, X. Li, and B. Yang, “A secure steganography: noisy region embedding,” in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009, pp. 1046–1051.

[29] W. Luo, F. Huang, and J. Huang, “Edge adaptive image steganography based on LSB matching revisited,” *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 201–214, 2010.

[30] J. Mielikainen, “LSB matching revisited,” *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May. 2006.