Journal of Computer and Communications, 2018, 6, 68-77
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Identity-Based Steganography in Spatial Domain

Xuba Xu*, **Qiankai Nie**

College of Information Science and Technology, Jinan University, Guangzhou, China
Email: *xuxuba36@sina.com

How to cite this paper: Xu, X.B. and Nie, Q.K. (2018) Identity-Based Steganography in Spatial Domain. *Journal of Computer and Communications*, **6**, 68-77.
https://doi.org/10.4236/jcc.2018.63005

Received: February 5, 2018
Accepted: March 20, 2018
Published: March 23, 2018

Abstract

This paper proposed an identity-based steganographic scheme, where a receiver with certain authority can recover the secret message ready for him, but cannot detect the existence of other secret messages. The proposed scheme created several separate covert communication channels tagged by the Fuzzy Identity-Based Encryption (FIBE) in one grayscale image. Then each channel is used to embed one secret message by using any content-aware steganographic scheme. Receivers with different attributes can extract different messages corresponded. The Experiments illustrated the feasibility of this identity-based secret message extraction. Further, the proposed scheme presents high undetectability against steganalytic attack launched by receivers without corresponded attributes.

Keywords

Steganography, Multiple Embedding, Fuzzy Identity-Based Encryption

1. Introduction

Steganography has been widely applied to secure communication especially in military espionage for a long time. It hides sensitive messages in a cover such as images. The redundancy of these covers is employed for embedding to avoid the hidden messages being detected. So existed steganaographic schemes absorb in improving the undetectability of the hidden messages against different kinds of steganalytic tools.

Steganalytic schemes at [1] [2] [3] [4] in spatial domain extract several sets of features from the cover, and then send them into the classifier such as [5] to analyze whether the test image conceals secret. In view of these, state-of-the-arts steganographic schemes mainly focus on exploring the undetectable region in an image. For example, schemes in [6] [7] extract the directional residuals of a cover image through filtering to define the textural region that is hard to model. Scheme in [8] [9] uses the multivariate Gaussian cover model to minimize the embedding distortion on statistics. What's more, thanks to the research of Syndrome-Trellis Codes (STC) [10], researchers no longer need to pay attention on the site of embedding, but only consider how to choose more appropriate distortion function.

Existed steganographic schemes only consider honest receivers and improve the entire security of the hidden messages. Due to the speciality of STC, every receiver with the knowledge of the existence of the hidden messages can extract all the secrets from the cover. However, some receivers may be corrupted in practice. If there are betrayers in the receivers, the secret will be leaked. What's more, secret messages are usually at specified sensitive levels, one cannot access, or even detect the existence of all these messages. If there are several messages at different security levels that want to be sent, existed steganographic schemes can only embed them into several covers to avoid secret leakage, which increases the communication cost. Additional information will also be necessary to distinguish different owners of these stego images. This is unsafe and inconvenient for practical secure communication.

In this paper, we propose a multiple embedding scheme by combining the Fuzzy Identity-Based Encryption [11] with the typical steganographic techniques. In our scheme, the sender can embed multiple messages associated with different attributes into one cover simultaneously, so that receivers extract the messages in accordance with their identity attributes. Each message needs a specific set of attributes to extract. For those attributes unmatched, receivers even won't know the existence of other embedded messages. In order to embed multiple messages, we generate masks for each message by using the FIBE based on their specific set of attributes. We embed messages according to their masks, and integrate them into one stego image. The receiver can locate the corresponding messages if and only if their identity attributes are matched, or they wouldn't know where or whether the messages are hidden.

There are various utilities for the proposed scheme. First, the embedded messages can be partially secure in the presence of corrupted receivers. As shown in the experiments, these receivers cannot detect the other embedded messages with their current knowledge. Second, a hierarchical extraction is available. Consider such a scenario where an operator receives a piece of digital works and finds that there are secret messages with the aid of his identity. He then forwards it to the persons concerned. The ones with higher-level identities can extract more messages, whose existence would not be known to the operator or the others.

The rest of this paper is organized as follows. Section 2 is to introduce the related works of our scheme. In Section 3, we will introduce our propose methods in detail. The experimental result will be show in Section 4 to compare our methods with current methods, and analyze the results. Finally, the paper is concluded in Section 5.

2. Related Works

2.1. Fuzzy Identity-Based Encryption

Fuzzy Identity-Based Encryption (FIBE) is a kind of public key cryptography. Its algorithm model designed is based on the Shamir's Secret Sharing [12] and bilinear pairings in cyclical group. The sender has a set of attributes and some of them are employ to encrypt the plain text, and only receivers whose attributes conform to the decryption attribute set can decrypt the cipher text. The specific steps of FIBE are described as following:

Setup(d). The authorized agency chooses random $y, t_1, \cdots, t_n \in \mathbb{Z}_q$. $\mathbb{Z}_q$ is a Galois field of prime number *q*. $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclical groups of *q*, they exist bilinear paring $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. The system public key PK is:

$$\left(Y = e(g,g)^y, T = g^t, \forall t \in \mathbb{Z}_q, g \in \mathbb{G}_1 \right)$$

Then the master key MK is:

$$(y, t_1, \cdots, t_n).$$

Key Generation. The authorized agency randomly chooses a $d-1$ times polynomial $p(x)$ satisfying $p(0) = y$. We suppose that $\mathcal{A}_u$ are the attributes of users. Then the private key of the user is:

$$\left(D = g^{\frac{p(i)}{t_i}}, \forall i \in \mathcal{A}_u \right).$$

Encryption. We supposed that $\mathcal{A}_c$ is the attribute set for decryption. Then the sender employs it to encrypt the secret $\in \mathbb{G}_2$. Randomly choosing $s \in \mathbb{Z}_q$, the cipher text is:

$$\left(\mathcal{A}_c, E = e(g,g)^{sy} M, E_i = g^{t_i s}, \forall i \in \mathcal{A}_c \right).$$

Decryption. When the receiver receives the cipher text, if $|\mathcal{A}_c \cap \mathcal{A}_u| > d$, he chooses *d* attributes out of $|\mathcal{A}_c \cap \mathcal{A}_u|$, and calculates $e(E_i, D_i) = e(g,g)^{p(i)s}$. We can find that:

$$Y^s = e(g,g)^{ys} = e(g,g)^{p(0)s}$$

according to the Lagrange interpolation formula. Then he can decrypt $M = E/Y^s$.

2.2. Steganographic Algorithm with Minimum Embedded Distortion

After embedding a certain amount of information, pixel values must change in spatial domain of secret images. The difference of pixel values existing between the cover image and the secret image, is generally called distortion. The quantization of image distortion is generally defined by the distortion function. The larger the value of the distortion function, the lower the security of the model.

The distortion function is usually expressed as a mathematical function. The distortion of additive distortion function is generally formed by the cumulative value of each pixel. The mathematical expression is generally expressed as:

$$D(X,Y)=\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}\rho_{i,j}\left(X,Y_{i,j}\right)\left|X_{i,j}-Y_{i,j}\right|,$$

n_1 and n_2 indicate how many pixels are in the horizontal and vertical columns of the cover image, and $X_{i,j}$ and $Y_{i,j}$ denote the values of the pixel corresponding to the i-th row and j-th column of the cover image respectively. $\rho_{i,j}$ represents the cost of changing the pixel value from $X_{i,j}$ to $Y_{i,j}$. The value of $\rho_{i,j}$ is determined by the cost function. The quality of the cost function determines the effect of information embedding. For example, the cost function of WOW [6] denoted as:

$$\rho_i=\sum_{\gamma=1}^{3}\left|\left|F^{(\gamma)}*X\right|*\left|F^{(\gamma)}\right|^{\curvearrowleft}\right|^{-1}$$

The wavelet bank is $F^{(1)}=h\cdot g^T$, $F^{(2)}=g\cdot h^T$, $F^{(3)}=g\cdot g^T$, g and h are respectively the low-pass and high-pass filters of the Daubechies 8 wavelet decomposition filter. $*$ represents the image filling convolution operation, $\curvearrowleft$ represents the matrix is rotated 90 degrees counterclockwise. After calculating the cost of each point, it is sent to the STC to get the embedded image.

3. Proposed Embedding Method

Our method is demonstrated in **Figure 1**. We choose one gray level image to embed multiple messages. Assume we have m messages to embed. To embed the i-th message, we use the i-th key to generate a mask using FIBE. Then the cover is divided into several regions according to the mask. The i-th message will be embedded into one region selected. After m rounds' embedding, all the m messages are embedded in the corresponded regions. By combining all the selected regions and the rest region of the image, we can reconstruct the stego image. The details are introduced in the following subsection.

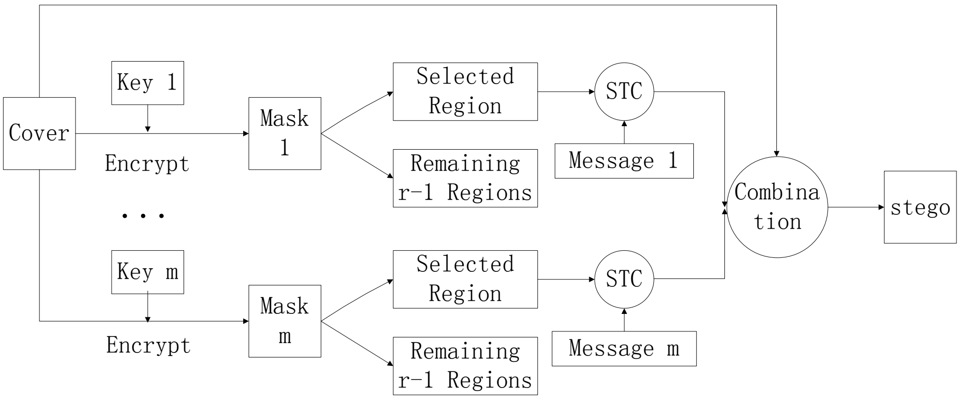


Figure 1. The overview of the proposed method.

3.1. Initialization

According to Section 2, we suppose that the sender has a set of attributes $\mathcal{A}u_S = \{Au_1, Au_2, \cdots, Au_N\}$, all the attributes employed to extract the mask are from this set. Assume the *m* messages that will be embedded are $\mathcal{M}_s = \{M_1, M_2, \cdots, M_m\}$. The attributes which can be used to extract the *i*-th mask are denoted as $\mathcal{A}u_{M_i} \subseteq \mathcal{A}u_S$. Supposing that $\mathcal{A}u_{M_i}$ has *k* attributes, any $j(j \le k)$ among *k* attributes of $\mathcal{A}u_{M_i}$ can extract the mask. We consider these *j* attributes as a threshold. Then the $\mathbb{Z}_q = \{t_1, t_2, \cdots, t_N\}$ are denoted as the manifold of $\mathcal{A}u_S$.

For the *i*-th message M_i, we choose the corresponding set $\mathbb{Z}_i \subseteq \mathbb{Z}_q$ of $\mathcal{A}u_{M_i}$ and a random $y_i \in \mathbb{Z}_q$. Let g_1 be a generator of $\mathbb{G}_1$. The public key of M_i is $\text{PK} = \left(Y_i = e(g_1, g_1)^{y_i}, T_i = g_1^{t_i}, \forall t_i \in \mathbb{Z}_i\right)$. The master key of M_i is $\text{MK} = (\mathbb{Z}_i, y_i)$.

For the receiver, we suppose he has a set of *j* attributes. We choose a random *j*-1 order function $p(x)$ satisfying $p(0) = y$. Then the secret key of the receiver is $\text{SK} = \left(D_j = g^{p(j)/t_j}, \forall j \in \mathbb{Z}_i\right)$.

3.2. Embedding

Suppose there are *m* messages to be embedded. We will introduce the procedure of embedding one message, saying, the *i*-th message. Label each pixel of the image with a unique integer *x* (Note that the receiver and sender have negotiated the label method). At first, we choose $g_2 \in \mathbb{G}_1$, and calculate $K_{(x)} = g_2^x$, which is the projection of the pixel in $\mathbb{G}_1$. Then we choose a random $s \in \mathbb{Z}_q$ and use $En_{i(x)} = e(g_1, g_1)^{sy_i} K_{(x)} mod\ r$, where *r* is the number of regions, to generate a mask $Mask_i = \left\{En_{i(x)}\right\}$ according to the labels of each pixel. By using this mask, we can divide the cover into r regions.

Secondly, we choose one of the *r* regions to embed the *i*-th message, denoted as $\mathcal{R}_i$. In this paper, we use the distortion function defined in WOW (Holub & Fridrich, 2012; Holub) to calculate the costs of changing pixels. Note that the employing of the distortion function is arbitrary. After that, to the pixels which do not belong to the selected region or belong to $\mathcal{R}_j, j \ne i$, we set their costs as $+\infty$. Then we employ STC to embed the *i*-th message into the cover and obtain a temporary stego image $\overline{I_i}$. Record the embedding modification $\Delta_i = \overline{I_i} - I$. It can be observed that all the nonzero elements in Δ_i are located in the selected region.

The procedures of embedding each message should be performed simultaneously, because calculating the cost of a pixel requires the selected regions associated with each message. After all the *m* messages have been embedded. We combine the modification as $\Delta = \sum_{i=1}^{I} \Delta_i$, and generate the final stego image by $\overline{I} = I + \Delta$.

At last, we send the stego image $\overline{I}$ along with the decryption attribute sets $\left(\mathcal{A}u_{M_i}, E_i = g_1^{t_i s}, \forall i \in \mathcal{A}u_{M_i}, g_2\right)$ to the receivers. The sets can be embedded in the stego image or sent in other secret ways. We will not discuss here.

3.3. Extraction

The extraction procedure is demonstrated in Figure 2. Unlike the decryption of FIBE, our scheme intends to locate the secret base on the plain text, but not to decrypt the secret.

After receiving the stego image, the receiver calculates $K_{(x)} = g_2^{S_{(x)}}$ according to subsection 3.2. We suppose his attribute set is $\mathcal{A}_r \subseteq \mathcal{A}u_S$, and the *i*-th message need *j* attributes to extract. If $\left|\mathcal{A}_r \cap \mathcal{A}u_{M_i}\right| \geq j$, the receiver can extract the *i*-th message. Then the receiver choose *j* attributes from $\mathcal{A}_r \cap \mathcal{A}u_{M_i}$, and calculate $e\left(E_i, D_i\right) = e\left(g_1, g_1\right)^{p(i)s}$. Then we have $Y_i^s = e\left(g_1, g_1\right)^{y_i s}$ according to the Lagrange interpolation formula. Finally, we can get $En_{i(x)} = Y_i K_{(x)}$ and the mask of *i*-th message. After dividing the stego image into *r* regions, we employ STC to extract the message from the selected region.

4. Experimental Result

4.1. Experiment Setup

To evaluate the performance of the proposed scheme, we employ 10,000 images of size 512 × 512 from the Boss Base 2 [13] as the test images. Pseudorandom binary sequences are employed as secret messages, which will be embedded in the stego images. These stego images are analyzed by the steganalytic features SRMQ (Fridrich & Kodovsky, 2012) combined with ensemble classifier (Kodovsky, Fridrich, & Holub, 2012). The OOB (out-of-bag) will be used as the secure index of steganographic schemes. At first, we combine the proposed scheme with the approaches WOW (Holub & Fridrich, 2012) and S-UINWARD (Holub, Fridrich, & Denemark, 2014) and compare the security between the proposed and the original. Secondly, we test the performances of varying the number of regions meanwhile fixing the total payload. Finally, we will test the security of the remained messages when some messages have been extracted.

4.2. Effectiveness Assessment

We suppose the region number is *r*, the message number is *m*. In each round, every region can employ 1/*r* of pixels to carry one message. Note that it is possible that averagely 1/*r* of the selected region's pixels appear at the regions selected in other *m*-1 rounds. To deal with this, we define the function of average maximal total payload (AMTP) as:

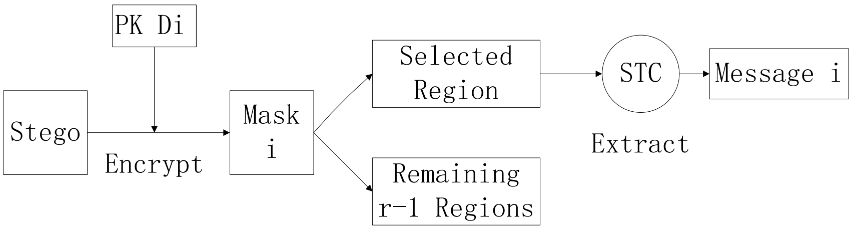


Figure 2. The extraction rules of the proposed method.

$$\text{AMTP} = m \times \frac{1}{r}\left(1 - \frac{1}{r}\right)^{m-1}. \tag{1}$$

ATMP represents the maximum total embedding payload that an image can embed in multiple messages in normal situation. According to Equation (1), we calculate the relationship of some situations as in Table 1. By choosing a suitable region number according to the message number, we can get a safe vocation for embedding. As a result, the message number is set as same as the region number in the propose method except noted.

Table 2 simulates some embedding situations. We embed the messages using different attributes sets, and test whether receivers have different attributes sets can extract the messages or not. It can be observed that only the receivers satisfied $\left|\mathcal{A}_r \cap \mathcal{A}u_{M_i}\right| \geq j$ can extract the *i*-th message.

Table 1. Average maximal total payload among messages of different region number.

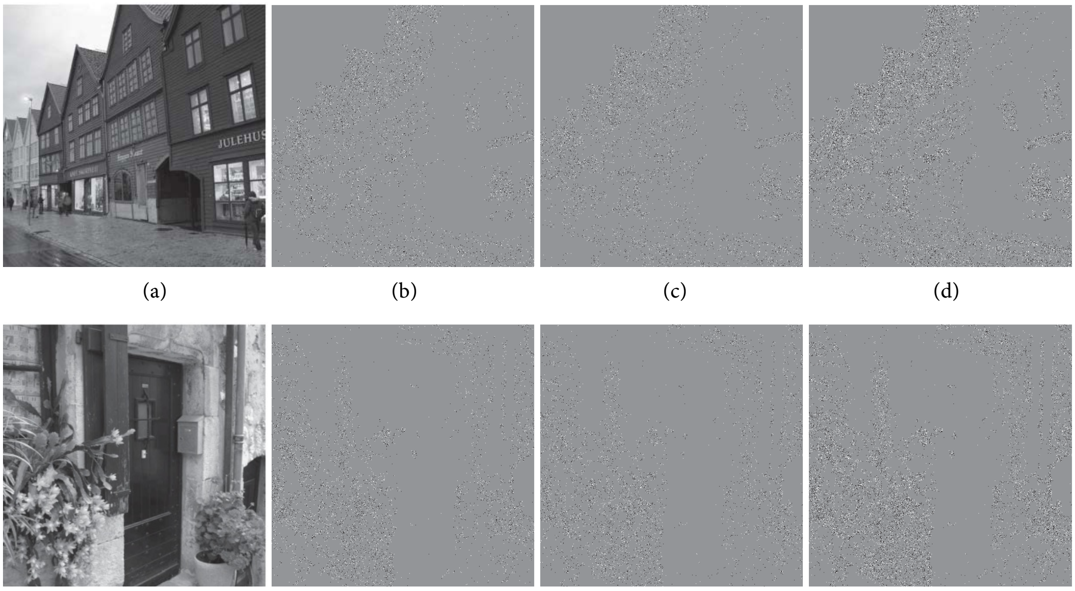
Region Message	2	3	4	5	6
2	**0.500**	0.444	0.375	0.320	0.278
3	0.375	**0.444**	0.422	0.384	0.347
4	0.250	0.395	**0.422**	0.410	0.386
5	0.156	0.329	0.396	**0.410**	0.402
6	0.094	0.263	0.356	0.393	**0.402**

Table 2. Truth table of attributes sets between receivers and messages.

$\mathcal{A}_r$ $\mathcal{A}u_{M_i}$	{1, 2}	{1, 3, 5}	{2, 3, 5}	{1, 4}	{1, 2, 3, 4, 5}
1 of {1, 4}	true	true	false	true	true
2 of {3, 5}	false	true	true	false	true
2 of {1, 4, 5}	false	true	false	true	true
3 of {2, 3, 5}	false	false	true	false	true
4 of {1, 2, 3, 4, 5}	false	false	false	false	true

In Figure 3, we can observe that the two messages embedded in one cover at the same time. The sites of the first message and second message are separated. What's more, the sites of embedding are all in the undetectable region defined by WOW. It makes the stego images secure against steganalytic attacks.

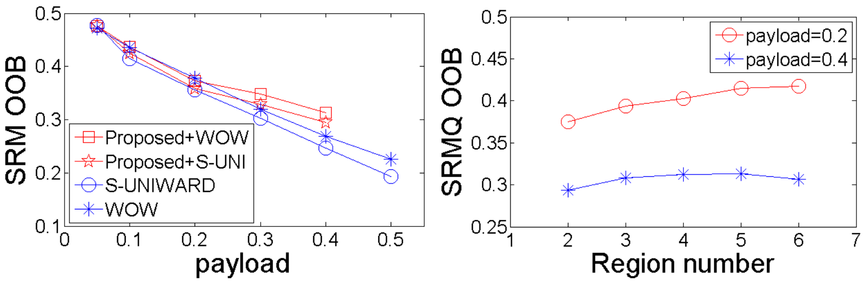
We use two distortion functions, namely WOW and S-UINWARD, to control the embedding distortions in the proposed scheme. The region number is set as 2. The securities of the proposed scheme and the original ones are compared in Figure 4(a) by using SRMQ. It can be observed that the performance of the proposed method is approximate to the original ones in the case of lower payload, and performs better when the payload is high. This is because the embedded feature based on the mask makes the position of the embedded point relatively random. Then the steganalytic scheme performing on the entire image is



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 3. (a) and (e) are two examples of test images from BossBase2, (b) and (f) are the embedding distortions incurred by embedding the first message, (c) and (g) are the embedding distortions incurred by the second message, (d) and (h) are the whole embedding distortions on the test images, here payload = 0.2 and N = 2. The white pixels represent embedding changes +1 and black pixels indicate embedding changes −1.

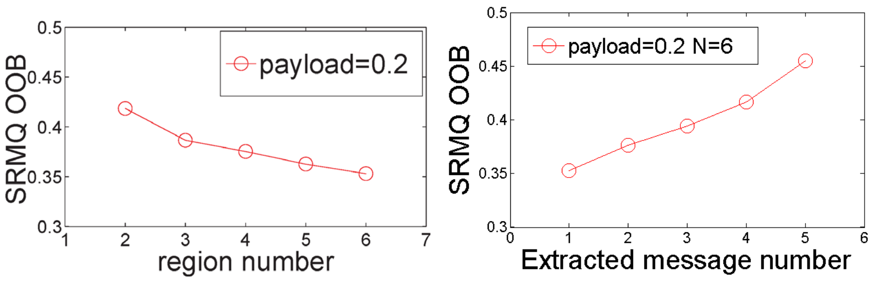


(a) (b)

Figure 4. Comparing security of identity-based embedding and other two general embedding method using the SRMQ (left) and Comparing security of different region number using the SRMQ (right).

more difficult to analyze the statistical features. So our scheme has a higher undetectability. Secondly, we compared the influence of different region numbers in the same payload in Figure 4(b). When $payload = 0.2$, we can observe that the more regions, the higher E_{OOB}. When $payload = 0.4$, the E_{OOB} will reduce instead if the region number is relative high. It is because increasing the regions would reduce the AMTP value.

In Figure 5(a), we observe that when one message has been extracted, the E_{OOB} of other messages stay in a high level. It means that if someone extracted one of the messages, he can hardly ensure whether there are other messages embedded or not. In Figure 5(b), we can observe that the more messages to extract, the higher E_{OOB} of the remained messages to get. It means that the security of the remaining messages will not reduce with more messages have been extracted.



(a)

(b)

Figure 5. When one message have been extracted, comparing the security of remained messages with respect to different region numbers with the same payload 0.2 (left).When different number of messages have been extracted, comparing the security of remained messages in the case of number of regions N = 6 and payload = 0.2 (right). SRMQ is used in the steganalytic method.

Instead, a higher undetectability is achieved.

5. Conclusions

In this paper, we introduce the risk of the receiver's unreliability, and present the idea of identity-based embedding. Based on the Fuzzy Identity-Based Encryption and WOW, we embed several messages simultaneously into one cover image. The receivers can only extract the message if his attributes is consistent. We first use the attributes set of *i*-th message to encrypt all the pixels of the cover image, and get the *i*-th mask to divide several regions. Then we employed one region to embed the *i*-th message after dealing with the cost of embedding.

By comparing with traditional methods, it can be observed that our proposed scheme is not inferior to them when embedding multiple messages in a low payload. When the payload is higher, our proposed scheme has more excellent experimental result. It is because that the unpredictability of regions copes with the steganalysis well. We also make a discussion between region number and message number, and analyze their average maximal total payload against security. Experiments support that the security of the remained messages will not be affected by knowing that some messages have been extracted.

Regarding the future work, we will try to improve the AMTP of our scheme by using other cryptography methods. Another potential improvement is expanding our scheme from spatial domain to other domains.

References

[1] Pevny, T., Bas, P. and Fridrich, J. (2009) Steganalysis by Subtractive Pixel Adjacency Matrix. *ACM Workshop on Multimedia and Security*, **5**, 75-84. https://doi.org/10.1145/1597817.1597831

[2] Fridrich, J. and Kodovsky, J. (2012) Rich Models for Steganalysis of Digital Images. *IEEE Transactions on Information Forensics* & *Security*, **7**, 868-882. https://doi.org/10.1109/TIFS.2012.2190402

[3] Holub, V. (2013) Random Projections of Residuals as an Alternative to Co-Occurrences in Steganalysis. *SPIE, Electronic Imaging, Media Watermarking, Security, and Fo-*

rensics, **8665**, 280-289. https://doi.org/10.1117/12.1000330

[4] Denemark, T., Fridrich, J. and Comesañaalfaro, P. (2016). Improving Selection-Channel-Aware Steganalysis Features. *Electronic Imaging*, No. 8, 1-8.

[5] Kodovsky, J., Fridrich, J. and Holub, V. (2012) Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Transactions on Information Forensics* & *Security*, **7**, 432-444. https://doi.org/10.1109/TIFS.2011.2175919

[6] Holub, V. and Fridrich, J. (2013) Designing Steganographic Distortion Using Directional Filters. *IEEE International Workshop on Information Forensics and Security*, **2**, 234-239.

[7] Holub, V., Fridrich, J. and Denemark, T. (2014) Universal Distortion Function for Steganography in an Arbitrary Domain. *Eurasip Journal on Information Security*, **2014**, 1. https://doi.org/10.1186/1687-417X-2014-1

[8] Fridrich, J. and Kodovský, J. (2013) Multivariate Gaussian Model for Designing Additive Distortion for Steganography. *IEEE International Conference on Acoustics, Speech and Signal Processing*, **32**, 2949-2953. https://doi.org/10.1109/ICASSP.2013.6638198

[9] Sedighi, V., Cogranne, R. and Fridrich, J. (2015) Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Transactions on Information Forensics & Security*, **11**, 221-234. https://doi.org/10.1109/TIFS.2015.2486744

[10] Filler, T., Judas, J. and Fridrich, J. (2011) Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. *IEEE Transactions on Information Forensics* & *Security*, **6**, 920-935. https://doi.org/10.1109/TIFS.2011.2134094

[11] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. *International Conference on Theory and Applications of Cryptographic Techniques*, **3494**, 457-473. https://doi.org/10.1007/11426639_27

[12] Shamir, A. (1984) Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology, Springer, Berlin.

[13] Bas, P., Filler, T. and Pevný, T. (2011) Break Our Steganographic System: The Ins and Outs of Organizing BOSS. *International Conference on Information Hiding*, **96**, 59-70. https://doi.org/10.1007/978-3-642-24178-9_5