A secure image steganography based on JND model

Tuan Duc Nguyen, Huu Dung Le
Faculty of Information Technology, Hanoi Open University, Hanoi, Vietnam

Article Info

Article history:

Received Sep 22, 2018
Revised Oct 28, 2019
Accepted Nov 5, 2019

Keywords:

Channel selection rule
Image steganography
Just noticeable difference model
Secure

ABSTRACT

Minimizing distortion produced by embedding process is very important to improve the security of hidden message and maintain the high visual quality of stego images. To achieve these objectives, an effective strategy is to perform pixel selection which is well-known as a channel selection rule. In this approach, a pixel associated with the smallest image degradation is chosen to carry secret bits. From these facts, in this paper, a new secure channel selection rule for digital images in spatial domain is designed and proposed. In this new approach, the modified matrix embedding method is utilized as data hiding method because it introduces more than one embedding change to be performed. This enables us to select a suitable pixel to embed message bits with less degradation yielded in a stego-image. In pixel selection of the proposed method, a just noticeable difference value and gradient value of a considering pixel are employed together. The experimental results (which were conducted on 10,000 uncompressed images) indicate that stego images of the proposed approach achieve a higher perceptual quality and security than those of the stego-images created by the previous approaches.

Corresponding Author:

Tuan Duc Nguyen,
Department of Information Systems,
Faculty of Information Technology, Hanoi Open University,
B101 Nguyen Hien street, Hai Ba Trung District, Hanoi, Vietnam.
Email: nguyenductuan@hou.edu.vn

1. INTRODUCTION

In the last decade, with the advance of network technology, a large amount of valuable information has been transferred over the Internet. Nevertheless, the confidentiality of these data can be broken without any protection in transmission process in a public network. Hence, cryptography is employed to protect these sensitive information and steganography can be used as an extra layer of security. In general, steganography techniques conceal confidential data into multimedia contents such as digital audio, video and image. Image is the most popular cover object employed to hide valuable data. There are two reasons for this. First, the digital image is very popular on the Internet. Second, we can alter redundant information of digital image to conceal secret message bits without causing any suspicions to human vision. This come from the fact that Human Vision System (HVS) is less sensitive to small changes on an image. In image steganography, a possibility to prevent a hidden message from being discovered by statistical steganalysis is the most important requirement [1]. Consequently, there are many image steganography methods (such as [2-4]) are developed to transfer valuable data in a secure way. Block based data hiding [5-11] and channel selection rule [1, 12-14] are two effective image steganography approaches for minimizing distortions to the cover images.

In block-based data hiding methods, such as matrix embedding (ME), an approach based Hamming code was developed by Crandall to minimize embedding changes [8]. It hides n secret bits to a cover block of $2^n - 1$ bits with only one bit in the block is altered. This method is then employed by Westfield in F5 algorithm [15]. However, only one embedding solution is introduced in ME. As a result, it cannot combine with channel selection rule techniques to further enhance the visual quality of the resulting images and security of the hidden messages. To obtain more embedding change solutions that can be selected to perform, Kim *et al.* [7] presented Modified Matrix Encoding (MME). Via this method, the introduced degradation is minimized by choosing an embedding solution that may cause less distortion to cover data. In general, MME schemes are named as MME2, MME3, etc., according to the maximum of modifications (*t*) which are required to hide *k* message bits to *n* cover bits [16].

For the channel selection rule approaches, these methods attempt to identify an image component's (a pixel in spatial domain or a transformed coefficient) that embedding secret bits into them cause less degradation. In channel selection rule approach for JPEG images introduced by Huang in [12], Quantization Step (QS) and magnitude of Discrete Cosine Transform (MQ), are concurrently considered with Perturbation Error (PE) to estimate an embedding distortion. The measured embedding error is utilized to determine embedding solutions to be performed in the data hiding process. Thus, the channel selection rule approaches can be combined with block-based data hiding methods (such as Hamming code based steganography techniques) [7] to improve the security of hidden data and obtain high visual quality stego-images.

For spatial images, several approaches have been presented [1, 13, 14, 17, 18] to enhance the visual quality of the stego-images and the security of a mysterious message. In two proposed methods [1, 17], a dissimilarity of considered pixel and its neighbors in value is estimated. After that, a characteristic (textured or smooth) of an image region that the considered pixel belongs to is identified based on the estimated value. If the pixel lies on complex image region, secret message bits are concealed in it. Otherwise, other pixels are used.

Luo *et al.* [13] proposed a data hiding scheme, in which the used image regions are identified based on the size of the secret message and the difference between two adjacent pixels. At low payloads, only pixels in complex regions are selected to carry message bits while maintaining the other flat regions as they are. When more message bits need to be embedded, more textured areas can be selected adaptively for data hiding by adjusting used parameters. Unfortunately, for the used image with large flat regions and the large payload is embedded, the less noisy regions are exploited to conceal the given secret message. This leads to the reduction of possibility to against visual and statistical attack methods.

To solve the above-mentioned facts, in [18], Nguyen *et al.* introduced a novel scheme in which a considered pixel's value and a difference between it and its neighbors are exploited to select a suitable pixel. Via this way, a visual quality of stego-images and the security of hidden message are enhanced. Unfortunately, image texture characteristic illustrates the large difference between pixels which does not include contrast and luminance. Luminance is illustrated as brightness; how bright an object appears to the human eye. While contrast is the dismissibility in visual characteristics that makes an object can be distinguished from other objects and the background. Two factors are used in Watson's visual model [19] which is applied to create a secure steganography method (proposed in [20]).

In this paper, a novel steganography scheme is proposed. In this approach the Just Noticeable Difference (JND) value is combined with a gradient (instead of using magnitude of a pixel as in [21]) to determine a pixel which need to be changed in data hiding process. This is due to the fact that hiding secret message bits in a pixel which has a corresponding JND value (measured by an approach in [22]) is higher than an altered value of pixel will cause less visible degradation. To examine the security of embedded message, regular/singular and ensemble classifier attack methods are performed. In these experiments, to further clarify the performance of the proposed approach, besides CBL [17], EALSBMR [13] is also used.

2. RESEARCH METHOD

In this section, a new image steganography scheme, which employs a novel channel selection rule to measure embedding distortion, is presented. In this approach, a corresponding embedding error of each solution (which is estimated by MME2) is calculated. Then, a solution which causes the smallest degradation to stego-image is selected to be performed in the data hiding process. As it can be seen in Figure 1, at sender's side, a secret message is hidden to the selected image by employing the proposed scheme. To send an image with a message embedded, a sender can use email services or upload it to public image sharing services, in which a stego image is kept as original. In addition, users can transfer these stego-images via social network services, such as Facebook. An uploaded image does not modify if user shares it through the upload file feature in the group's wall.

In this proposed approach, a JND value is calculated and then used to estimate embedding noise. The reason is that JND employs enhanced contract masking (CM) estimation with better edge masking (EM) and texture masking (TM) calculation [22]. Moreover, if the value of a pixel is changed with a quantity which is smaller than its corresponding JND value, the introduced distortion is invisible to HVS. To further enhance a security of hidden message, a new criterion average gradient (AG) of a pixel is utilized.

It is integrated with JND value (which is calculated by a method in [22]) to measure embedding distortion. This is an improvement of new approach in comparison with proposed method in [21]. The reason is that pixel associated with large gradient value may belong to textured image regions, and those with small values may be located on flat regions. While a large value of pixel cannot indicate the complexity of the region it belongs to.

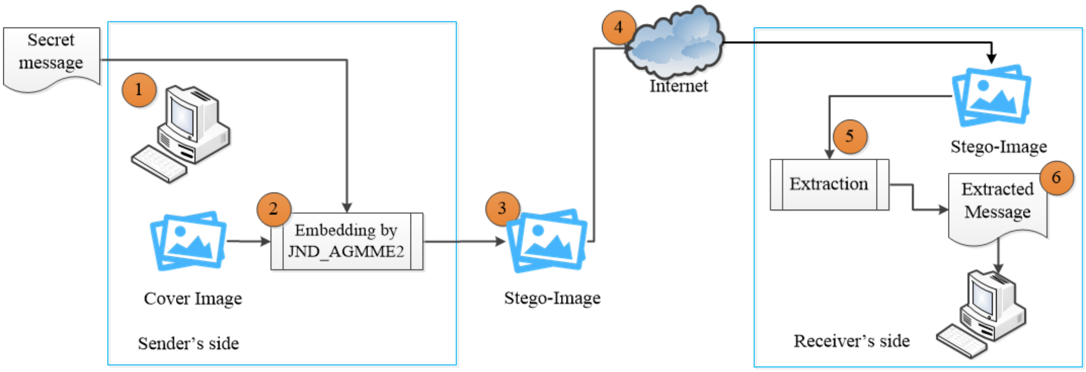


Figure 1. A JND model based steganography scheme

An embedding distortion is estimated as follows:

$$E_{i,j} = (J_{i,j})^{\alpha_1} / (AG_{i,j})^{\alpha_2} \tag{1}$$

where $J_{i,j}$ is a JND value and $AG_{i,j}$ is an average gradient of pixel (i, j). Note that, in case the gradient value of considered pixel ($AG_{i,j}$) equals to zero, it will be set to 10^{-3} to avoid dividing by zero. Two non-negative parameters α_1 and α_2 are employed to examine the effect of provided factors JND and AG (which is calculated by Equation (3) in [1]) to image visual quality and security of hidden message.

To further increase the security of hidden message, the schemes of MME2 (in which two modifications are required) is utilized as an embedding method in the proposed scheme (named as JND_AGMME2). This is because MME2 provides more than one possible bit-change choices to be performed. In this proposed approach, embedding distortion is calculated (by Equation (1)) in each solution (introduced by MME2) and the one associated with the smallest error is performed to carry given message bits. To summarize, MME2 exhibits "how" to embed and the proposed channel selection rule shows "where" to hide secret message bits. Consequently, the application of the proposed approach is presented as follows.

Given a message block of k bit $M = (m_1, m_2,\ldots,m_k)$ to hide in a block of cover pixels $P = (p_1, p_2,\ldots,p_n)$ with $n = 2^k - 1$ pixels. A value of k is estimated according to the size of given message and cover image. This strategy enables us to split message bits evenly spread out to stego-image. As a result, for a small number of message bits, there are more cover pixels which will be used in block P. In contrast, when an embedding rate increased, the number of pixels in the block P is reduced. Therefore, there are more employed blocks to guarantee that all given message bits are embedded.

A message block M is concealed into the block of pixels P by performing three following steps:

Step 1. A value ρ is calculated by $H * BL^T - M^T$ with BL (a block contains LSBs of pixels in P) and $[.]^T$ is transpose operator. After that the pairs (β, γ) that satisfy $\beta \oplus \gamma = \rho$ are listed. As mentioned above, there are $(n - 1)/2$ pairs of pixels can be enumerated.

Step 2. For each pair (β, γ) in the enumerated list, a total corresponding embedding error is estimated by Equation (1). Assume that E_ρ is the noise caused by modifying LSB of a pixel at position ρ, then we denote $E_{(\beta_{min}, \gamma_{min})}$ is the smallest measured embedding distortion of the pairs (of pixels) in the enumerated list.

Step 3. If $E_\rho < E_{(\beta_{min}, \gamma_{min})}$ then pixel ρ is altered, otherwise the pair of pixels $(\beta_{min}, \gamma_{min})$ are modified to carry M. The selected pixel is changed by the following equation (which is derived from [18]):

Case #1: if $(P_i = 255) \| (P_i = 0)$ then

$$P_i = \begin{cases} P_i = P_i - 1 & if (P_i = 255) \\ P_i = P_i + 1 & if (P_i = 0) \end{cases} \tag{2}$$

Case #2: if (P_i > 0 && P_i < 255) then

$$P_i = \begin{cases} P_i = P_i - 1 & if(rand < 0.5) \\ P_i = P_i + 1 & if(rand \geq 0.5) \end{cases} \tag{3}$$

where i is the position of a pixel in P is modified to conceal message bits. To improve the security of secret message against statistical steganalysis methods (such as Regular/Singular – RS [20]), in (3), a Matlab's function ***rand*** is used to add or subtract value of the selected pixels by 1 randomly. At the receiver side, a hidden message is extracted by performing $M = H * BLS'$ where BLS is a block of LSBs of stego pixels.

3. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

This section describes the experimental results and compares the algorithm performance of the proposed approach with other previous approaches. In the experiments, a public image database, Break Our Watermarking System (BOWS) is employed as test image database. This image library contains 10,000 natural gray-scale images, each of whose sizes are all 512 x 512 pixels with different characteristics. To use in the experiments, the PGM images in BOWS were converted to BMP image file format via **imwrite** function of Matlab. In the following experiments, the message with various embedding payloads ranging from 0.05 to 0.40 *bpp* with a step of 0.05 *bpp* is concealed into cover images by the proposed approach JND_AGMME2 and three existing methods (AG_MME, the techniques presented in [1], EALSBMR [13] and CBL [17]). The employed messages are generated randomly to make the ratio of bit 1 and 0 is balanced. This plays an important role to avoid creating uniform regions in stego-images. It is because in the proposed approach, the cover pixels are determined also based on the value of message bits.

3.1. Embedding capacity and visual quality discussion

For available embedding capacity, the proposed scheme exploits MME2 as an embedding method. Hence, it offers the same embedding capacity as the previous based MME2 methods. In this perceptual quality experiment, the images from BOWS are divided into five segments. Then generated message with payload in the range of [0.05 – 0.40] *bpp* is embedded into these divided segments. Later, the images with message embedded are analyzed for Peak signal-to-noise ratio (PSNR) to examine visual quality. Generally, the higher PSNR value, the lesser is the degradation in stego-images [24]. Average PSNR values, which were measured from cover images and their corresponding stego-images produced by the proposed approach (JND_AGMME2) with different embedding rates of secret message, were presented in Table 1. From Table 1, it is observed that the obtained average PSNR values of stego-images when the two parameters α_1, α_2 > 0 are higher than those of stego-images produced by the proposed approach with other values of α_1 and α_2 for most of the embedding capacities. In these cases, both criteria JND and AG are utilized to estimate embedding noise (by (4)). In the possible embedding solutions (yielded by MME2), the one associating with the smallest distortion (embedding noise) is altered in the embedding process.

Table 1. Average PSNR values of 10,000 stego-images by the proposed approach (JND_AGMME2) under different embedding rates and value of two used parameters

	PSNR (in dB)					
bpp	α_1=0.0,	α_1=0.5,	α_1=0.2,	α_1=0.5,	α_1=0.0,	α_1=1.0,
	α_2=0.5	α_2=0.0	α_2=0.5	α_2=0.2	α_2=1.0	α_2=0.0
0.05	69.6908	69.6730	69.6903	69.6936	69.6750	69.2627
0.10	65.3249	65.3194	65.3242	65.3256	65.3188	65.1226
0.15	63.5638	63.5586	63.5635	63.5649	63.5574	63.3514
0.20	61.4879	61.4868	61.4882	61.4893	61.4845	61.3567
0.25	60.5186	60.5175	60.5190	60.5198	60.5155	60.3875
0.30	58.7777	58.7778	58.7779	58.7785	58.7764	58.7180
0.35	58.1088	58.1084	58.1086	58.1090	58.1063	58.0477
0.40	57.5287	57.5283	57.5292	57.5292	57.5269	57.4678

As demonstrated results in Table 2, the proposed scheme offers better stego-image quality than those of the three previous methods (AG_MME2, EALSBMR, and CBL). This enhancement is obtained by integrating JND with AG of the considered pixel to estimate the embedding distortion caused by the data hiding process. For example, at small embedding rates (from 0.05 to 0.20 *bpp*), the visual quality of stego-images produced by the proposed approach extremely outperforms the other methods (CBL and EALSBMR). The reason is that at low embedding rate, according to the principle of the proposed approach there are more pixels utilized to embed the same as number of secret message bits in comparison with the cases which high embedding rates are used. This strategy supports to obtain more modification solutions can be performed in data hiding. As a result, the high perceptual quality is achieved.

PSNR metric only takes into account the difference between an original and modified pixels not degradation in structure of an image. Therefore, to examine the degradations in structural information introduced by data hiding to stego-images, a structural similarity index (SSIM) [25], an effective method in measuring the similarity between two images (original and modified), is utilized. In SSIM, three factors loss of correlation, luminance distortion, and contrast distortion, are employed. Therefore, it is suitable to measure structural degradations of stego-images produced by the proposed approach. The higher SSIM value is, the small distortion in the structural information of stego-image is.

Table 2. Visual quality comparison (illustrated by PSNR values) of the proposed approach and three existing methods (AG_MME2, CBL, and EALSBMR) under different embedding rates

bpp	PSNR (in dB)							
	$\alpha_1 = 0.0, \alpha_2 = 0.5$		$\alpha_1 = 0.2, \alpha_2 = 0.5$		$\alpha_1 = 0.5, \alpha_2 = 0.2$		CBL	EALSBMR
	AG_MME2	JND_AGMME2	AG_MME2	JND_AGMME2	AG_MME2	JND_AGMME2		
0.05	69.5554	69.6908	69.2069	69.6903	68.4291	69.6936	62.4646	65.3091
0.10	65.2851	65.3249	65.0524	65.3242	64.5762	65.3256	59.4548	62.2974
0.15	63.5180	63.5638	63.3094	63.5635	62.8342	63.5649	57.7102	60.5371
0.20	61.4692	61.4879	61.3025	61.4882	60.9840	61.4893	56.4801	59.2877
0.25	60.4986	60.5186	60.3445	60.5190	60.0275	60.5198	55.5199	58.3182
0.30	58.7718	58.7777	58.6462	58.7779	58.4776	58.7785	54.7320	57.5263
0.35	58.1016	58.1088	57.9852	58.1086	57.8153	58.1090	54.0532	56.8573
0.40	57.5223	57.5287	57.4110	57.5292	57.2423	57.5292	53.4767	56.2770

Table 3 reveal that the SSIM values of stego-images produced by the proposed scheme JND_AGMME2 are higher than those of the previous method AG_MME2 for high embedding rates (from 0.35 to 0.40 *bpp*) when both of the two parameters α_1, $\alpha_2 > 0$. This performing can be archived because JND_AGMME2 compares embedding distortion caused by one-modification solutions with that of two modifications required solutions to select an optimal solution (a solution introduced the smallest noise). Moreover, in the proposed scheme, employing JND in embedding distortion measurement is an effective way to maintance the structure of stego-images. From Table 3, for the embedding payload from 0.05 to 0.20 *bpp*, the stego-images created by the proposed method illustrates a higher degradation in structural information than those of CBL. The reason for this is that, in CBL, to reduce the number of required embedding changes, a preprocess was performed. It sets LSBs of all image pixels to zero. Hence, if a secret bit is zero, no modification is applied.

Table 3. Comparison of average SSIM over 10,000 stego-images produced by the proposed approach and the three previous methods

bpp	SSIM							
	$\alpha_1 = 0.0, \alpha_2 = 0.5$		$\alpha_1 = 0.2, \alpha_2 = 0.5$		$\alpha_1 = 0.5, \alpha_2 = 0.2$		CBL	EALSBMR
	AG_MME2	JND_AGMME2	AG_MME2	JND_AGMME2	AG_MME2	JND_AGMME2		
0.05	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9998
0.10	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9999	0.9997
0.15	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9995
0.20	0.9996	0.9996	0.9996	0.9996	0.9995	0.9996	0.9996	0.9993
0.25	0.9995	0.9995	0.9995	0.9995	0.9994	0.9995	0.9994	0.9991
0.30	0.9992	0.9992	0.9992	0.9992	0.9991	0.9992	0.9992	0.9990
0.35	0.9991	0.9991	0.9991	0.9991	0.9990	0.9991	0.9990	0.9988
0.40	0.9990	0.9990	0.9989	0.9990	0.9989	0.9990	0.9987	0.9986

When the payloads were set to the range of [0.25 – 0.40] *bpp*, the number of required changes has increased to hide a secret message. Therefore, the stego-images of CBL cannot maintain a low distortion in terms of structure. Hence, Table 3 shows that SSIM values of stego-images generated by CBL are smaller than those values of stego-images produced by JND_AGMME2 for all payloads. In comparison with EALSBMR, JND_AGMME2 maintenances a better quality in structural of stego-images under various of used embedding rates. This result is because EALSBMR uses the difference of the considered pixel and its neighbor to determine whether the considered pixel located on complex regions or not. If an absolute difference is higher than a predefined threshold *T*, then the two considering consecutive pixels are used to conceal secret message bits. Unfortunately, after embedding this approach need to readjust the value of stego pixels to guarantee the difference between the two pixels is higher than threshold *T*. As a result, the change in structural of the stego images created by EALSBMR is higher than that of the proposed approach.

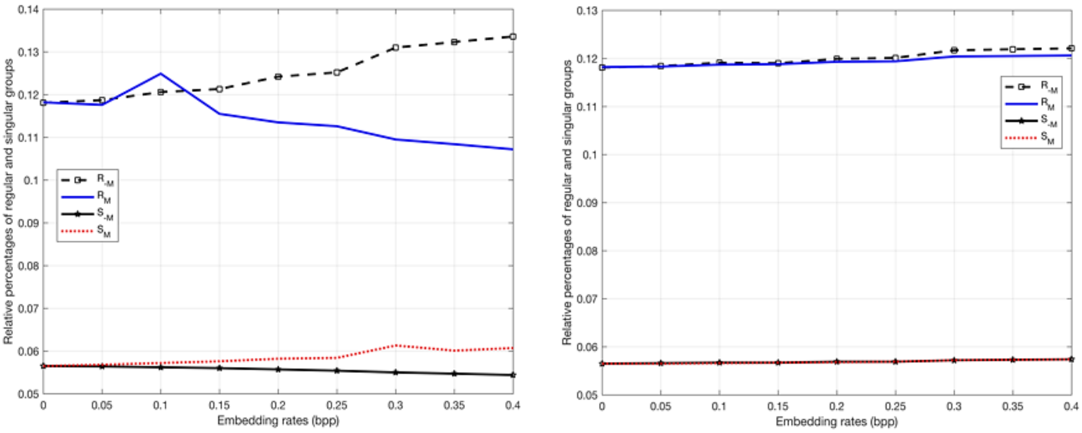
3.2. Security analysis

a. Regular/singular attack

As a rule, employing the LSB of pixels to conceal secret message bits causes the statistical changes of images. However, this distortion is invisible to HVS and LSB Enhancement is ineffective in discovering a hidden message if the given message is embedded into edge pixels. Hence, in this subsection, to reliably and accurately determine the existence of a mysterious message hidden by the proposed approach, Regular/Singular steganalysis introduced by Fridrich *et al.* is employed [23].

In this test, a discrimination function and a flipping operation are used to identify three groups of pixels Regular (R), Singular (S) and Unchanged (U). In general, the identification of these groups express on how the flipping changes the value of discrimination function [26]. To evaluate the size of secret message, the relative number of two groups is measured for the cover image and stego-image. The obtained results are represented in RS diagram with four-dimensional RS features (R_M, R_{-M}, S_M, S_{-M}) and *M* is flipping mask. As a rule, if a suspected stego image contains a secret message, the difference (in value) between features in the pair (R_M, R_{-M}) and (S_M, S_{-M}) becomes larger when the embedding rate is increased [23].

To examine the security against RS steganalysis method of stego-images by the JND_AGMME2 and AG_MME2, the value of two groups in pairs (R_M versus R_{-M}, S_M versus S_{-M}) were plotted in Figure 2. As it can be seen in Figure 2(a), it is obviously the higher data embedded, the larger dissimilarity of these groups is. Contrary to AG_MME2, the relation of two groups in pairs in RS diagram (Figure 2(a)) is steady unchanged even a large amount of message is hidden into stego-images by JND_AGMME2. This means that JND_AGMME2 is robust to RS steganalysis. It can be observed that the randomly change of pixels in value to carry message bits supports to remain the difference between these two groups in pairs as same as in cover images.



(a) (b)

Figure 2. (a) RS diagram of stego-images produced by AG_MME2 and (b) JND_AGMME2

b. Security against ensemble classifier

In this subsection, we conduct an experiment to clarify the security against Ensemble Classifier (an universal steganalysis based on feature set) [27] of the proposed approach. In this experiment, feature set (including 1183 features) was extracted from each stego-image in divided segments by content-selective residuals (CSR) [28] extractor, to be used in Ensemble classification. Out-of-bag (OOB) value is the testing error introduced by Ensemble Classifier. Typically, the large OOB value indicates that the steganography techniques can achieve a high security against Ensemble Classifier. Based on demonstrated results in Figure 3, the security of JND_AGMME2 is significantly superior to three existing approaches (AG_MME2, EALSBMR, and CBL) with payload is in the range of [0.05 – 0.40] *bpp* and various values of the two used parameters (α_1, α_2). The reason is that in JND_AGMME2 two factors were utilized in data hiding error measurement. For the first criterion JND, the modifications with a changed value (of pixel) which is smaller than the estimated JND value will cause less statistical noise than that of others. The high value of the second criterion AG illustrates that the considered pixel locates in a complex region of image. That is obviously employing JND and AG supports to reduce the possibility to be detected by Ensemble Classifier (illustrated as high OOB errors). From the Table 4, it can be seen that with various values of the two used parameters, the stego-images are produced with different security levels (illustrated by OOB errors). The security against Ensemble Classifier is higher when the two parameters are non-zero. In other words, the possibility to detect the existence of hidden message embedded by the proposed approach with the combination of gradient and JND by Ensemble Classifier steganalyzer is reduced.

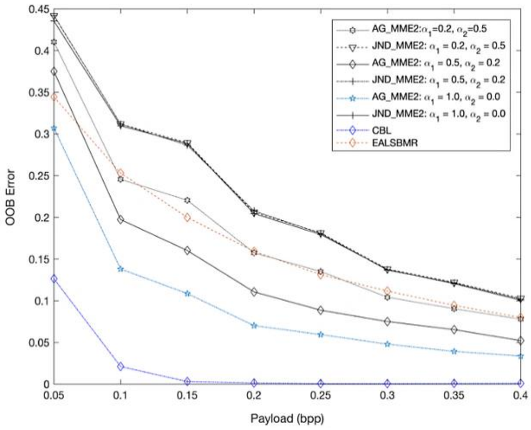


Figure 3. Comparision of security of stego-images produced by JND_AGMME2 and previous methods against Ensemble classifier

Table 4. Testing error OOB of JND_AGMME2 against CSR feature set under different values were set to two parameters α_1 and α_2

	OOB error					
bpp	α_1=0.0 α_2=0.5	α_1=0.5 α_2=0.0	α_1=0.2 α_2=0.5	α_1=0.5 α_2=0.2	α_1=0.0 α_2=1.0	α_1=1.0 α_2=0.0
0.05	0.4372	0.4331	0.4418	0.4421	0.4425	0.4354
0.10	0.3114	0.3040	0.3118	0.3118	0.3073	0.3097
0.15	0.2866	0.2837	0.2893	0.2864	0.2845	0.2884
0.20	0.2067	0.2045	0.2060	0.2077	0.2038	0.2045
0.25	0.1825	0.1792	0.1814	0.1807	0.1822	0.1794
0.30	0.1389	0.1368	0.1379	0.1367	0.1372	0.1373
0.35	0.1184	0.1219	0.1220	0.1213	0.1235	0.1205
0.40	0.1018	0.0997	0.1028	0.1018	0.0998	0.1005

4. CONCLUSION

This paper proposed a secure channel selection rule-based steganography approach in spatial domain. Two factors JND and AG are combined to estimate embedding degradation since JND reveals the minimum visible threshold of HVS. While AG supports to identify the texture characteristic of image region which the considered pixel belongs to. Therefore, the security of stego-images, produced by the new scheme, against statistical steganalysis methods is enhanced. In the experiments conducted, although CSR (the feature extractor with 1183 features) is employed instead for SPAM (including 686 features) in Ensemble Classifier, the security of the proposed approach still overcomes the previous approaches. In addition, RS analysis fails to detect the existence of mystery message embedded into stego-images by the proposed approach. The proposed approach also offers high perceptual quality images proved by obtained experimental results.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial support of Hanoi Open University for this research. We would like to thank our colleagues from Faculty of Information Technology, Hanoi Open University who provided valuable suggestions that greatly assisted the research.

REFERENCES

[1] Y. Zhong, F. Huang, and D. Zhang, "New Channel Selection Criterion for Spatial Domain Steganography," in *Digital Forensics and Watermaking*, vol. 7809, Y. Q. Shi, H.-J. Kim, and F. Pérez-González, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–7, 2013.

[2] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in Image Hiding using Developed LSB and Random Method," *Int. J. Electr. Comput. Eng. IJECE*, vol. 8, no. 4, p. 2091, Aug. 2018.

[3] W. A. Shukur and K. K. Jabbar, "Information Hiding using LSB Technique based On Developed PSO Algorithm," *Int. J. Electr. Comput. Eng. IJECE*, vol. 8, no. 2, p. 1156, Apr. 2018.

[4] S. Khan and T. Bianchi, "Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region," *Int. J. Electr. Comput. Eng. IJECE*, vol. 8, no. 1, p. 379, Feb. 2018.

[5] Q. Mao, "A fast algorithm for matrix embedding steganography," *Digit. Signal Process.*, vol. 25, pp. 248–254, Feb. 2014.

[6] C. Wang, W. Zhang, J. Liu, and N. Yu, "Fast Matrix Embedding by Matrix Extending," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 346–350, Feb. 2012.

[7] Y. Kim, Z. Duric, and D. Richards, "Modified Matrix Encoding Technique for Minimal Distortion Steganography," in *Information Hiding*, vol. 4437, J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 314–327, 2007,.

[8] R. Crandall, "Some Notes on Steganography," 1998.

[9] T. Yang and H. Chen, "Matrix embedding in steganography with binary Reed–Muller codes," *IET Image Process.*, vol. 11, no. 7, pp. 522–529, 2017.

[10] G. Liu, W. Liu, Y. Dai, and S. Lian, "Adaptive steganography based on block complexity and matrix embedding," *Multimed. Syst.*, vol. 20, no. 2, pp. 227–238, Mar. 2014.

[11] A. Sarkar, U. Madhow, and B. Manjunath, "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography," *Inf. Forensics Secur. IEEE Trans. On*, vol. 5, pp. 225–239, 2010.

[12] F. Huang, J. Huang, and Y.-Q. Shi, "New Channel Selection Rule for JPEG Steganography," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 4, pp. 1181–1191, Aug. 2012.

[13] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 201–214, Jun. 2010.

[14] K.-H. Jung and K.-Y. Yoo, "Data hiding using edge detector for scalable images," *Multimed. Tools Appl.*, vol. 71, no. 3, pp. 1455–1468, Aug. 2014.

[15] A. Westfeld, "F5—A Steganographic Algorithm," in *Information Hiding*, vol. 2137, I. S. Moskowitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 289–302, 2001.

[16] F. Huang, W. Luo, J. Huang, and Y.-Q. Shi, "Distortion function designing for JPEG steganography with uncompressed side-image," *Proceedings of the 2013 ACM Information Hiding and Multimedia Security Workshop*, 2013, pp. 69-76.

[17] V. Sabeti, S. Samavi, and S. Shirani, "An adaptive LSB matching steganography based on octonary complexity measure," *Multimed. Tools Appl.*, vol. 64, no. 3, pp. 777–793, Jun. 2013.

[18] T. D. Nguyen, S. Arch-int, and N. Arch-int, "A novel secure channel selection rule for spatial image steganography," in *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 2015, pp. 230–235.

[19] A. B. Watson, "DCT quantization matrices visually optimized for individual images," *Proceedings of SPIE - The International Society for Optical Engineering*, 1913–14, pp. 202–216, 1993.

[20] M. Fakhredanesh, R. Safabakhsh, and M. Rahmati, "A Model-Based Image Steganography Method Using Watson's Visual Model," *ETRI J.*, vol. 36, no. 3, pp. 479–489, Jun. 2014.

[21] Tuan Duc Nguyen and Huu Dung Le, "A new secure steganography method for grayscale images in spatial domain based on Just Noticeable Difference model," in *The 19th National Symposium of Selected ICT Problems*, Ha Noi, pp. 14–20, 2016.

[22] A. Liu, W. Lin, M. Paul, C. Deng, and F. Zhang, "Just Noticeable Difference for Images With Decomposition Model for Separating Edge and Textured Regions," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 11, pp. 1648–1652, Nov. 2010.

[23] J. Fridrich, M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images," *IEEE Multimed.*, vol. 8, pp. 22–28, 2001.

[24] H.-H. Liu and C.-M. Lee, "High-capacity reversible image steganography based on pixel value ordering," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, p. 54, Apr. 2019.

[25] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Measurement to Structural Similarity," *IEEE TRANS IMAGE Process.*, vol. 13, pp. 600–612, 2004.

[26] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, "Quantitative steganalysis of digital images: estimating the secret message length," *Multimed. Syst.*, vol. 9, no. 3, pp. 288–302, Sep. 2003.

[27] J. Kodovsky, J. Fridrich, and V. Holub, “Ensemble Classifiers for Steganalysis of Digital Media,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 432–444, Apr. 2012.

[28] T. Denemark, J. Fridrich, and V. Holub, “Further study on the security of S-UNIWARD,” *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 9028 p. 902805, 2014.

BIOGRAPHIES OF AUTHORS

Tuan Duc Nguyen has received the PhD degree in Computer Science from Khon Kaen University (KKU), Khon Kaen, Thailand, in 2016. He received the M.SC degree from Le Qui Don Technical Univeristy, Vietnam in 2008. He is currently working as a lecturer in Faculty of Information Technology, Hanoi Open University, Hanoi, Vietnam. His research interests are cryptography, steganography and cloud computing. Contact him at nguyenductuan@hou.edu.vn

Huu Dung Le has received the M. Sc degree in Applied Mathematics for Information Technology from VNU University of Science, Hanoi, Vietnam since 2015. He is currently a lecturer of Faculty of Information Technology, Hanoi Open University, Hanoi, Vietnam. His research interests are security and data science. Contact him at huudungle@hou.edu.vn