A secure image steganography based on JND model

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

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,
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 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:

\[ E_{i,j} = \left( J_{i,j} \right)^{\alpha_1} / \left( AG_{i,j} \right)^{\alpha_2} \]  \hspace{1cm} (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 \( 10^{-1} \) to avoid dividing by zero. Two non-negative parameters \( \alpha_1 \) and \( \alpha_2 \) 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_AGMMME2). 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 \( \rho \) is calculated by \( H \ast BL^T - M^T \) with \( BL \) (a block contains LSBs of pixels in \( P \)) and \( \lfloor . \rfloor^T \) is transpose operator. After that the pairs \((\beta, \gamma)\) 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 \((\beta, \gamma)\) in the enumerated list, a total corresponding embedding error is estimated by Equation (1). Assume that \( E_\rho \) is the noise caused by modifying LSB of a pixel at position \( \rho \), then we denote \( E_{\rho_{\min}, \gamma_{\min}} \) is the smallest measured embedding distortion of the pairs (of pixels) in the enumerated list.

**Step 3.** If \( E_\rho < E_{\rho_{\min}, \gamma_{\min}} \) then pixel \( \rho \) 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]):

\[
\text{Case #1: if } (P_i = 255) \text{ or } (P_i = 0) \text{ then } \\
P_i' = \begin{cases} 
P_i = P_i - 1 & \text{if } (P_i = 255) \\
P_i = P_i + 1 & \text{if } (P_i = 0) 
\end{cases}
\]  \hspace{1cm} (2)

The algorithm performance of 5 to 0.20 ≠ ≥ − ·− 𝑃 𝑛 generated message with 0 − 1 𝑖𝑓 𝐵𝐿𝑆 𝑖𝑓 ME2) The reason is that at low embedding rate, according to the principle of the proposed approach there are more images produced by the proposed approach extremely outperforms the other methods (CBL and EALSBMR). This enhancement is obtained by embedding noise) is altered in the embedding process. 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. The parameter 𝛼 > 0 are higher than those of stego-images produced by the proposed approach with other values of 𝛼1 and 𝛼2 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_AGME2) under different embedding rates and value of two used parameters

<table>
<thead>
<tr>
<th>bpp</th>
<th>ℿ1=0.0, ℿ2=0.0</th>
<th>ℿ1=0.5, ℿ2=0.0</th>
<th>ℿ1=0.2, ℿ2=0.0</th>
<th>ℿ1=0.2, ℿ2=0.5</th>
<th>ℿ1=0.0, ℿ2=0.0</th>
<th>ℿ1=1.0, ℿ2=0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05</td>
<td>69.6908</td>
<td>69.6730</td>
<td>69.6903</td>
<td>69.6936</td>
<td>69.6750</td>
<td>69.2627</td>
</tr>
<tr>
<td>0.10</td>
<td>65.3249</td>
<td>65.3194</td>
<td>65.3242</td>
<td>65.3256</td>
<td>65.3188</td>
<td>65.1226</td>
</tr>
<tr>
<td>0.15</td>
<td>63.5638</td>
<td>63.5586</td>
<td>63.5635</td>
<td>63.5649</td>
<td>63.5574</td>
<td>63.3514</td>
</tr>
<tr>
<td>0.20</td>
<td>61.4879</td>
<td>61.4868</td>
<td>61.4882</td>
<td>61.4893</td>
<td>61.4845</td>
<td>61.3567</td>
</tr>
<tr>
<td>0.25</td>
<td>60.5186</td>
<td>60.5175</td>
<td>60.5190</td>
<td>60.5198</td>
<td>60.5155</td>
<td>60.3875</td>
</tr>
<tr>
<td>0.30</td>
<td>58.7777</td>
<td>58.7778</td>
<td>58.7779</td>
<td>58.7785</td>
<td>58.7764</td>
<td>58.7180</td>
</tr>
<tr>
<td>0.35</td>
<td>58.1088</td>
<td>58.1084</td>
<td>58.1086</td>
<td>58.1090</td>
<td>58.1063</td>
<td>58.0477</td>
</tr>
<tr>
<td>0.40</td>
<td>57.5287</td>
<td>57.5283</td>
<td>57.5292</td>
<td>57.5292</td>
<td>57.5269</td>
<td>57.4678</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>bpp</th>
<th>$\alpha_1 = 0.0$, $\alpha_2 = 0.5$</th>
<th>PSNR (in dB)</th>
<th>$\alpha_1 = 0.2$, $\alpha_2 = 0.5$</th>
<th>$\alpha_1 = 0.5$, $\alpha_2 = 0.2$</th>
<th>CBL</th>
<th>EALSBMR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
</tr>
<tr>
<td>0.05</td>
<td>69.3554</td>
<td>69.6008</td>
<td>69.2099</td>
<td>69.6905</td>
<td>68.4291</td>
<td>69.6936</td>
</tr>
<tr>
<td>0.10</td>
<td>65.2851</td>
<td>65.3249</td>
<td>65.0524</td>
<td>65.3242</td>
<td>64.5762</td>
<td>65.3256</td>
</tr>
<tr>
<td>0.15</td>
<td>63.5180</td>
<td>63.5638</td>
<td>63.3094</td>
<td>63.5635</td>
<td>62.8342</td>
<td>63.5649</td>
</tr>
<tr>
<td>0.20</td>
<td>61.4692</td>
<td>61.4879</td>
<td>61.3025</td>
<td>61.4882</td>
<td>60.9840</td>
<td>61.4893</td>
</tr>
<tr>
<td>0.25</td>
<td>60.4986</td>
<td>60.5186</td>
<td>60.3445</td>
<td>60.5190</td>
<td>60.0275</td>
<td>60.5198</td>
</tr>
<tr>
<td>0.30</td>
<td>58.7718</td>
<td>58.7777</td>
<td>58.6462</td>
<td>58.7779</td>
<td>58.4776</td>
<td>58.7785</td>
</tr>
<tr>
<td>0.35</td>
<td>58.1016</td>
<td>58.1088</td>
<td>57.9852</td>
<td>58.1086</td>
<td>57.8153</td>
<td>58.1090</td>
</tr>
<tr>
<td>0.40</td>
<td>57.5223</td>
<td>57.5287</td>
<td>57.4110</td>
<td>57.5292</td>
<td>57.2423</td>
<td>57.5299</td>
</tr>
</tbody>
</table>

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 $\alpha_1$, $\alpha_2 > 0$. 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 mantaince 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

<table>
<thead>
<tr>
<th>bpp</th>
<th>$\alpha_1 = 0.0$, $\alpha_2 = 0.5$</th>
<th>SSIM</th>
<th>$\alpha_1 = 0.2$, $\alpha_2 = 0.5$</th>
<th>SSIM</th>
<th>$\alpha_1 = 0.5$, $\alpha_2 = 0.2$</th>
<th>SSIM</th>
<th>CBL</th>
<th>EALSBMR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
<td>JND_AGMME2</td>
<td>AG_MME2</td>
</tr>
<tr>
<td>0.05</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>0.10</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
<td>0.9998</td>
</tr>
<tr>
<td>0.15</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
<td>0.9997</td>
</tr>
<tr>
<td>0.20</td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9995</td>
<td>0.9995</td>
<td>0.9995</td>
<td>0.9995</td>
</tr>
<tr>
<td>0.25</td>
<td>0.9995</td>
<td>0.9995</td>
<td>0.9995</td>
<td>0.9995</td>
<td>0.9994</td>
<td>0.9994</td>
<td>0.9994</td>
<td>0.9994</td>
</tr>
<tr>
<td>0.30</td>
<td>0.9992</td>
<td>0.9992</td>
<td>0.9992</td>
<td>0.9992</td>
<td>0.9991</td>
<td>0.9991</td>
<td>0.9991</td>
<td>0.9991</td>
</tr>
<tr>
<td>0.35</td>
<td>0.9991</td>
<td>0.9991</td>
<td>0.9991</td>
<td>0.9991</td>
<td>0.9990</td>
<td>0.9990</td>
<td>0.9990</td>
<td>0.9990</td>
</tr>
<tr>
<td>0.40</td>
<td>0.9990</td>
<td>0.9990</td>
<td>0.9989</td>
<td>0.9990</td>
<td>0.9989</td>
<td>0.9990</td>
<td>0.9990</td>
<td>0.9987</td>
</tr>
</tbody>
</table>

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.

![Figure 2](image)

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 ($\alpha_1$, $\alpha_2$). 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.

![Comparison of security of stego-images produced by JND_AGMM2E and previous methods against Ensemble classifier](image)

**Figure 3. Comparison of security of stego-images produced by JND_AGMM2E and previous methods against Ensemble classifier**

**Table 4. Testing error OOB of JND_AGMM2E against CSR feature set under different values were set to two parameters $\alpha_1$ and $\alpha_2$.**

<table>
<thead>
<tr>
<th>$b$</th>
<th>$\alpha_1$</th>
<th>$\alpha_2$</th>
<th>$b$</th>
<th>$\alpha_1$</th>
<th>$\alpha_2$</th>
<th>$b$</th>
<th>$\alpha_1$</th>
<th>$\alpha_2$</th>
<th>$b$</th>
<th>$\alpha_1$</th>
<th>$\alpha_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05</td>
<td>0.4372</td>
<td>0.4331</td>
<td>0.4418</td>
<td>0.4421</td>
<td>0.4425</td>
<td>0.4354</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.10</td>
<td>0.3114</td>
<td>0.3040</td>
<td>0.3118</td>
<td>0.3118</td>
<td>0.3073</td>
<td>0.3097</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.15</td>
<td>0.2866</td>
<td>0.2837</td>
<td>0.2893</td>
<td>0.2864</td>
<td>0.2845</td>
<td>0.2884</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.20</td>
<td>0.2067</td>
<td>0.2045</td>
<td>0.2060</td>
<td>0.2077</td>
<td>0.2038</td>
<td>0.2045</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>0.1825</td>
<td>0.1792</td>
<td>0.1814</td>
<td>0.1807</td>
<td>0.1822</td>
<td>0.1794</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.30</td>
<td>0.1389</td>
<td>0.1368</td>
<td>0.1379</td>
<td>0.1367</td>
<td>0.1372</td>
<td>0.1373</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.35</td>
<td>0.1184</td>
<td>0.1219</td>
<td>0.1220</td>
<td>0.1213</td>
<td>0.1235</td>
<td>0.1205</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.40</td>
<td>0.1018</td>
<td>0.0997</td>
<td>0.1028</td>
<td>0.1018</td>
<td>0.0998</td>
<td>0.1005</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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


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 University, 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