Protecting Secret Data using RDE and Fuzzy Logic to Specify the Embedding Level

Ahmad Junior Ilham
Department of Informatics
Institut Teknologi Sepuluh Nopember
Kampus ITS, Surabaya, Indonesia
juniar.18051@mhs.its.ac.id

Puti Harum Bawa
Software Engineer
PT Bukalapak.com
Jakarta, Indonesia
lightharum.108@gmail.com

Tohari Ahmad
Department of Informatics
Institut Teknologi Sepuluh Nopember
Kampus ITS, Surabaya, Indonesia
tohari@if.its.ac.id

Abstract—Along with the rapid increase in information technology, there is a challenge in data security. For this reason, data protection has been a focus for some decades. One of the methods, called data hiding, is introduced to solve this security issue. It can protect secret data; nevertheless, the quality of the resulted stego data for a certain amount of the secret is limited. Moreover, the reversibility of the algorithm is also a concern. In this research, we intend to improve the method by combining Reduced Difference Expansion (RDE) and the concept of fuzzy logic, by considering some factors, such as brightness and its entropy value. It is to specify the number of embedding, which should be done for each block in an image. Therefore, the embedding level is dynamic, which means that it may be different for each block. The experimental result shows that this proposed method works well; adaptive such that it follows the characteristics of the carrier. Moreover, the method is also reversible that both the secret data and the carrier can be successfully reconstructed.

Index Terms—data hiding, data protection, data security, image processing

I. INTRODUCTION

The technology, especially information and communication technology (ICT), has been a key factor in doing many financial activities for decades. It is because most of the transactions depend on the availability of this high-computing technology. For example, the operation of the bank highly relies on the security of the data. Moreover, nowadays, most of the financial transactions can be done at any place and time. Therefore, the disruption of ICT operation in the monetary process may cause many losses.

Nevertheless, these advantages have some flaws which can be exploited by illegitimate users. For example, they may carry out information phishing and identity theft. In more details, the secret data being transferred may be intercepted and modified by an attacker. In this case, the security of the data has been compromised. It means that the data are not confidential anymore; additionally, their integrity is not maintained.

Some methods have been implemented to solve that security issue, depending on the characteristics of the data and the environment. It includes the data hiding method which protects the secret data by embedding them to a particular medium, called the carrier or the cover. It can be an image, audio, video, or text. By embedding the secret into this carrier, it may not be found easily by the attacker. In a further implementation, the secret can be firstly encrypted before being embedded, but it may cause a more complicated process.

The data hiding itself, still has some challenges, especially the amount of the secret which can be hidden; and the quality of the generated stego data. Another factor which is also considered is the reversibility [1], where the intended recipient can reconstruct both the secret and the medium. At least, the secret must be extractable. It means that it is compulsory that the secret can be obtained successfully. Some other important factors are imperceptibility and fidelity. Imperceptibility means the existence of the secret message cannot be perceived by the public; while fidelity means the quality of cover media does not change much due to insertion. In general, the imperceptibility and the fidelity relate to the quality of the stego data.

In order to avoid misperception of the extracted secret due to the quality of the generated medium, it is necessary to choose a method that can reconstruct the cover to its original form after the secret message is received. One of the popular methods is the reversible data hiding, such as Difference Expansion (DE) [2] and its variations like Reduced Difference Expansion (RDE) [1] [3]. It is a development of DE method, which pays attention much on the quality of the stego data. Indirectly, it also means increasing the capacity of the secret, which can be embedded for a certain quality level. In its development, the data hiding methods can be combined with many intelligence algorithms such as Particle Swarm Optimizer (PSO), Adaptive Neural Networks (ANN), and Genetic Algorithms (GA).

Ashraf et al. [4] proposed a type-2 fuzzy logic-based interval system to detect pixels of images that are less sensitive to the human eye. In that research, the embedding process uses the Least Significant Bit (LSB). Saleema and Amarunnishad [5] proposed new steganography using Hybrid Neural Network to improve the capacity of the embedding secret data while maintaining excellent image quality.

Generally, the purpose of this combination is to achieve the maximum results and adaptive solutions. Several developments have been carried out, such as [4] which combines RDE and Fuzzy Logic (FL) for determining the embedding level. However, this method still uses LSB in the process of inserting data;
Fig. 1. Embedding process

and, the original cover may not be recovered. To overcome this problem, we propose to combine a data hiding method with fuzzy logic for increasing imperceptibility by using an image as the cover. In this algorithm, the RDE is employed instead of the LSB.

The structure of this paper is as follows. Section 2 describes the previous research that has been conducted. Section 3 explains the proposed method. Section 4 represents the experimental results, and the conclusion is depicted in the last section.

II. RELATED WORKS

The concept of DE has been the base of some extended data hiding methods, which include [1] [2] [6]. In 2008, Lou et al. [2] used RDE to prevent stego quality from significant reduction. Furthermore, it is also to avoid both the underflow and overflow by implementing the multiple layer embedding. In this case, overflow and underflow mean that the reconstructed pixel value is more than 255 and less than 0, respectively. Their proposed method can improve the performance; however, it does not process pairs of pixels containing a negative difference.

In 2013, Sajasi and Moghadam [3] proposed an initial stage of the adaptive steganography scheme based on the Fuzzy Inference System (FIS) to determine the number of bits inserted in a block, whose size is $3 \times 3$ pixels. The characteristics of the blocks are used as the input to fuzzy logic, which are the texture, edge sensitivity, and brightness. It implements the LSB-based embedding method. When a block has a more coarse texture, and the edge sensitivity value increases, the number of bits that can be inserted per pixel also increases. Similarly, when the brightness of a block is high, the number of bits inserted also rises.

Next, Ahmad et al. [1] conducted a study to enhance the PSNR and the capacity of the secret data by improving quad RDE. Their research shows an increase of 4.8 dB in PSNR with a slightly higher secret message capacity. They claim that their method produces higher values than the previous ones. The research in [6] proposed a data hiding approach using an Enhanced Reduced Difference Expansion (E-RDE) and pixel blocks to improve the previous research in [1]. In the experiments, they suggest using blocks whose size is $4 \times 1$ (vector) by scanning images vertically. The embedding process of the secret data in a reduced difference is calculated between the closest pixels in each block.

III. PROPOSED METHOD

This section describes the general description of the method, embedding design, and bit extraction. Besides, the design of the method for determining the embedding level in multi-layer insertion is also provided.

A. General Description

The proposed method lies in the mechanism of determining the embedding level. This insertion level is applied to multi-layer RDE methods, where it specifies the maximum number of layers that can be inserted in a block. In this design, each block contains $2 \times 2$ pixels.

Each block has different insertion levels, where the process of calculating the level for each block uses fuzzy logic. The characteristics of each block have become inputs that are processed using fuzzy logic whose final result is the block level value.

Fig. 2. Structure of the blocks
B. Overall Method Scheme

The initial stage in the proposed scheme is the same as the initial stage in an adaptive steganography scheme based on the fuzzy inference system (FIS) proposed by Sajasi and Moghadam [3]. Different from it, where the texture, edge sensitivity, and LSB-based brightness are the focus, in this research, we consider other factors to be the input to the fuzzy logic. This dissimilarity is caused by the difference between the LSB and the RDE insertion method. As a result, the initial stage of the scheme produces a fuzzy inference system that is not the same as that suggested by [3].

In the multi-layer insertion section, this method adopts the procedure proposed by Lou et al. [2]. In that method, scanning is done to get the pixel pairs of an image. Like [2], we propose to scan the image both horizontally and vertically; differently, we use $2 \times 2$ of blocks, instead of $3 \times 3$. Then, insertion is done according to the insertion level of each block, which is obtained from the fuzzy logic method. The multi-layer RDE embedding procedure using fuzzy logic is presented in Fig. 1.

C. Bit Embedding and Bit Extraction

In this research, we employ the RDE embedding method similar to that of Lou et al. [2]. Different from that research which does not process pairs of pixels with a negative difference, in this paper, we combine it with that of Ahmad et al. [1]. It is to process the embedding and bit extraction by using RDE in case that the resulting difference is negative. It is intended to make the cover image recoverable in the extraction process.

D. Multi-Layer Embedding

In the multi-layer embedding, a design is made on how to scan blocks, map level structure, method of ordering pixel pairs, and designing the location map. The illustration of a block structure is provided in Fig. 2. In more details, it shows a block consisting of pixels 1, pixels 2, pixels 3 and pixels 4.

The data block is obtained by scanning the cover image. The sequence of blocks scanning in an image is shown in Fig. 3. Here, the scanning is done horizontally. The same number indicates that the pixel belongs to the same block, and the respective number is to be the existing block pointer index.

Similar to other methods, a map is required to store the information of each block. It is developed according to the characteristics of the corresponding block. The embedding level determines the maximum amount of hiding that can be done on the block. This map is in the form of arrays, where the column indicates block indexes. The total block can be calculated by $M \times N/4$, where $M \times N$ is the image size.

An example of a level map of an image with $4 \times 4$ pixels is depicted in Fig. 4.

Based on this level map, an expandable block list is generated. This list of expandable blocks shows which blocks are embeddable for the particular layer. Also, this list is in the form of 2-dimensional arrays, whose column shows the block indexes and the row is the order of layers in the multi-layer embedding. Here, the number of rows is obtained from the highest embedding level value. An example of an expandable block list is presented in Fig. 5, which is developed based on the map in Fig 4.

There are many combinations of sequence pairs of pixels that can be designed for multi-layer embedding by using RDE. In this research, we demonstrate the horizontal and vertical sequence. Similar to the level map, the location map is in the form of a two-dimensional array. The number of rows indicates the number of the embedding layer; while the columns show the number of pixel pairs in the image whose total pixel pair can be calculated by $M \times N/2$, where $M \times N$ is the image size.

E. Embedding Level

In the multi-layer embedding process, the quality of the stego image is predicted to be lower according to the number
of layers being applied. The purpose of determining the level of multi-layer embedding is to maintain the quality of the stego image. The design of this mechanism can be described as follows.

1) Fuzzy Variable: We propose several block characteristics as the fuzzy variables. These characteristics indicate how close the distance or relationship between pixels in a block. For this purpose, we include some factors: local brightness, local entropy, local distance, and local standard deviation of the block. The local brightness value is the average of pixel values in a block. The local entropy is the average local entropy of each pixel in a block. Similarly, the value of local distance and the local standard deviation is the average value of all pixels in a block.

2) Fuzzification and Fuzzy Membership Functions: From the process of the embedding data in a block, we can determine the fuzzy membership function, which consists of the characteristics of a predetermined block. Some values are set, such that the local brightness membership is between 0 and 255; that of local entropy is between 0 and 4; that of the local conversation and domain membership functions are between 0 to 255. Finally, the functions of the standard deviation is between 0 and 150. Then, the insertion level value as fuzzy output has a universe and domains from 0 to 8.3.

In the fuzzy membership function, we use a trapezoidal curve which has 4 points, as depicted in Fig. 6. They are indicated by \(a, b, c\) and \(d\). Point \(a\) and \(b\) depict the smallest domain value that has zero and one membership degrees, respectively. Point \(c\) and \(d\) show the most substantial domain value that has correspondingly one and zero membership degree.

IV. EXPERIMENTAL RESULTS

To evaluate the proposed method, we use four testing images to be the cover taken from [7] [8] as depicted in Fig. 7. As shown, they are grayscale images whose size is 512 \(\times\) 512 pixels. In this evaluation, we measure the similarity level between the original cover image and the resulted stego image. For this purpose, the Peak Signal to Noise Ratio (PSNR) represented in dB is used, where the higher value means the better quality.

Furthermore, various sizes of secret have been applied: 1kb, 10kb, 20kb, 30kb, 40kb, and 50kb. This secret is in the form of random binary numbers, and the result of the experiment is provided in Table I. It is shown that the use of entropy gives the best effect on the quality of the stego image. For example, by using entropy in a small secret message (i.e., 1kb), the highest PSNR is achieved by Abdominal, which is around 70dB. Similarly, this cover also has the highest PSNR for each considered factor. On the other hand, Baboon is the lowest. For each considered factor, Baboon is still the lowest for all secret sizes.

In general, increasing the size of the message leads to decreasing the PSNR value. It happens to all factors and cover images. The amount of this decrease is almost the same for each factor to the corresponding cover image. The highest drop is experienced by Baboon when the size rises from 1kb to 10kb. It can reduce about 10dB; at the same condition, Abdominal goes up from 40kb to 50kb, which is relatively high, Baboon has the lowest drop (i.e., about 1dB); while the others have about 2dB, although its PSNR is still the lowest.

It can be inferred that the characteristics of Abdominal are more appropriate to use for various secret sizes. In terms of the considered factors, entropy is better to use than others. For the comparison, we also implement the method of Lou et al. [2] whose result is provided in Table II.

According to Tables I and II, we find that in general, the proposed method has better results except the Abdominal. In this case, the difference is about 5dB. It is worth noting that Abdominal is a medical image which mostly darker than others; while the others are standard images.
TABLE I

THE QUALITY OF THE STEGO IMAGE GENERATED BY THE PROPOSED METHOD WITH VARIOUS SECRET SIZES

<table>
<thead>
<tr>
<th>Factor</th>
<th>Cover Image</th>
<th>PSNR (dB) 1kb</th>
<th>PSNR (dB) 10kb</th>
<th>PSNR (dB) 20kb</th>
<th>PSNR (dB) 30kb</th>
<th>PSNR (dB) 40kb</th>
<th>PSNR (dB) 50kb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightness</td>
<td>Baboon</td>
<td>53.904</td>
<td>44.468</td>
<td>42.6789</td>
<td>40.9232</td>
<td>40.2524</td>
<td>39.9024</td>
</tr>
<tr>
<td></td>
<td>Boat</td>
<td>66.061</td>
<td>54.3525</td>
<td>52.7573</td>
<td>50.1082</td>
<td>46.3442</td>
<td>44.2517</td>
</tr>
<tr>
<td></td>
<td>Pepper</td>
<td>66.0201</td>
<td>55.0873</td>
<td>53.6074</td>
<td>51.0415</td>
<td>47.9874</td>
<td>46.9541</td>
</tr>
<tr>
<td></td>
<td>Abdominal</td>
<td>67.7057</td>
<td>59.2389</td>
<td>56.7642</td>
<td>55.3436</td>
<td>52.5652</td>
<td>50.3442</td>
</tr>
<tr>
<td>Entropy</td>
<td>Baboon</td>
<td>54.3898</td>
<td>45.8165</td>
<td>43.4526</td>
<td>42.0295</td>
<td>41.9272</td>
<td>40.8188</td>
</tr>
<tr>
<td></td>
<td>Boat</td>
<td>66.0816</td>
<td>54.7091</td>
<td>52.0678</td>
<td>49.6379</td>
<td>48.6392</td>
<td>46.9372</td>
</tr>
<tr>
<td></td>
<td>Pepper</td>
<td>66.2546</td>
<td>55.6188</td>
<td>53.9207</td>
<td>49.7452</td>
<td>48.4366</td>
<td>47.3379</td>
</tr>
<tr>
<td></td>
<td>Abdominal</td>
<td>70.5437</td>
<td>62.7632</td>
<td>59.5232</td>
<td>59.3232</td>
<td>57.9292</td>
<td></td>
</tr>
<tr>
<td>Range</td>
<td>Baboon</td>
<td>54.1054</td>
<td>45.3897</td>
<td>43.1654</td>
<td>41.9364</td>
<td>40.9731</td>
<td>39.8244</td>
</tr>
<tr>
<td></td>
<td>Boat</td>
<td>66.0641</td>
<td>54.3523</td>
<td>52.0427</td>
<td>49.6592</td>
<td>48.6392</td>
<td>46.9372</td>
</tr>
<tr>
<td></td>
<td>Pepper</td>
<td>66.0978</td>
<td>55.3938</td>
<td>53.7074</td>
<td>51.7445</td>
<td>48.6888</td>
<td>47.5741</td>
</tr>
<tr>
<td></td>
<td>Abdominal</td>
<td>69.6543</td>
<td>61.6389</td>
<td>59.6342</td>
<td>58.8336</td>
<td>58.5652</td>
<td>56.9942</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>Baboon</td>
<td>54.3898</td>
<td>45.8165</td>
<td>43.4526</td>
<td>42.0295</td>
<td>41.9272</td>
<td>40.8188</td>
</tr>
<tr>
<td></td>
<td>Boat</td>
<td>66.0816</td>
<td>54.7091</td>
<td>52.0678</td>
<td>49.6379</td>
<td>48.6392</td>
<td>46.9372</td>
</tr>
<tr>
<td></td>
<td>Pepper</td>
<td>66.2689</td>
<td>55.6469</td>
<td>53.8233</td>
<td>51.7423</td>
<td>49.7324</td>
<td>47.3145</td>
</tr>
<tr>
<td></td>
<td>Abdominal</td>
<td>70.4627</td>
<td>62.6894</td>
<td>60.6323</td>
<td>59.4728</td>
<td>59.2516</td>
<td>57.8264</td>
</tr>
</tbody>
</table>

TABLE II


<table>
<thead>
<tr>
<th>Method</th>
<th>Cover Image</th>
<th>PSNR (dB) 1kb</th>
<th>PSNR (dB) 10kb</th>
<th>PSNR (dB) 20kb</th>
<th>PSNR (dB) 30kb</th>
<th>PSNR (dB) 40kb</th>
<th>PSNR (dB) 50kb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lou et al. [2]</td>
<td>Baboon</td>
<td>53.0404</td>
<td>44.4676</td>
<td>42.8767</td>
<td>40.9232</td>
<td>40.2524</td>
<td>39.9024</td>
</tr>
<tr>
<td></td>
<td>Boat</td>
<td>65.9694</td>
<td>53.8298</td>
<td>49.9994</td>
<td>47.3744</td>
<td>45.344</td>
<td>43.865</td>
</tr>
<tr>
<td></td>
<td>Pepper</td>
<td>66.0631</td>
<td>55.131</td>
<td>51.6207</td>
<td>49.4292</td>
<td>48.0375</td>
<td>47.0356</td>
</tr>
<tr>
<td></td>
<td>Abdominal</td>
<td>75.7202</td>
<td>65.5537</td>
<td>62.4471</td>
<td>60.7542</td>
<td>59.953</td>
<td>57.9256</td>
</tr>
</tbody>
</table>

V. CONCLUSION

In this paper, we have proposed a method for protecting secret data. Here, the fuzzy logic is applied by considering some factors: brightness, entropy, range, and standard deviation. The proposed method also overcomes the problem happening in the previous research, where a negative difference value may not be processed.

It is necessary to design membership functions for accurate input and output variables to increase PSNR and imperceptibility of stego images. The membership function can determine the embedding level of a pixel pair. With this embedding level, pixel pairs that can reduce PSNR drastically will not be processed, while the rest have an embedding rate according to the characteristics of each pixel block.

REFERENCES