



Improving the Reversible LSB Matching Scheme Based on the Likelihood Re-Encoding Strategy

Tzu-Chuen Lu ^{1,*}, Ping-Chung Yang ¹ and Biswapati Jana ²

¹ Department of Information Management, Chaoyang University of Technology, Taichung 41349, Taiwan; s10814617@cyut.edu.tw

² Department of Computer Science, Vidyasagar University, Midnapore 721102, India; biswapatijana@gmail.com

* Correspondence: tclu@cyut.edu.tw

Abstract: In 2018, Tseng et al. proposed a dual-image reversible embedding method based on the modified Least Significant Bit matching (LSB matching) method. This method improved on the dual-image LSB matching method proposed by Lu et al. In Lu et al.'s scheme, there are seven situations that cannot be restored and need to be modified. Furthermore, the scheme uses two pixels to conceal four secret bits. The maximum modification of each pixel, in Lu et al.'s scheme, is two. To decrease the modification, Tseng et al. use one pixel to embed two secret bits and allow the maximum modification to decrease from two to one such that the image quality can be improved. This study enhances Tseng et al.'s method by re-encoding the modified rule table based on the probability of each hiding combination. The scheme analyzes the frequency occurrence of each combination and sets the lowest modified codes to the highest frequency case to significantly reduce the amount of modification. Experimental results show that better image quality is obtained using our method under the same amount of hiding payload.

Keywords: dual imaging technique; reversible data hiding; least-significant-bit matching; re-encoding technique



Citation: Lu, T.-C.; Yang, P.-C.; Jana, B. Improving the Reversible LSB Matching Scheme Based on the Likelihood Re-Encoding Strategy. *Entropy* **2021**, *23*, 577. <https://doi.org/10.3390/e23050577>

Academic Editor: Sotiris Kotsiantis

Received: 12 April 2021

Accepted: 27 April 2021

Published: 8 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the rapid development of digital technology nowadays, a large amount of information is transmitted on the Internet. Although it is convenient, it is also, however, insecure. The transmitted data may be stolen by unscrupulous third parties. Consequently, to keep the seed details from being tampered with or viewed, researchers use different information-hiding techniques to conceal and cover the information transmitted over unsecured channels. There are three major requirements for information-hiding methods, as follows [1]:

- (1) **Security:** This requirement is necessary to protect the information from being detected or cracked by illegitimate third parties.
- (2) **Imperceptibility:** To improve protection, the image cannot be blurred, deformed, or distorted, and cannot be easily detected by the human eye.
- (3) **High Capacity:** The more data embedding, the higher the distortion that occurs. Making good use of every hidden space, and increasing the capacity are also important.

Information-hiding technologies can be classified into “Reversible Data Hiding (RDH)” and “Non-Reversible Data Hiding (NRDH).” Most of the early information-hiding technologies are NRDH, meaning that after extracting the confidential information, there is no way to restore it to the original image, such as with the Least Significant Bit Replacement (LSB), LSB matching, modulus methods, and so on. However, scholars have successively proposed various RDH techniques to fix this problem. Nowadays, researchers are working hard on increasing the hiding capacity and improving the visual quality, which is also the standard for measuring the quality of the suggested method [2,3].

The RDH schemes focus on the image quality and whether it can be restored in the future, so the RDH method usually uses a lower amount of secret information. Increasing the capacity of RDH storage has become one of the challenges that have been paid much attention to in recent years. Common RDH methods include the Difference Expansion, Histogram Shifting, Compression Image and Dual-Images (DI) techniques, and so on [4–13].

Some RDH methods are essentially reversible, while some become reversible after being improved by certain techniques [14–17]. Among them, the LSB matching method, which was proposed by Mielikainen in 2006, uses the parity of the Least Significant Bit value of pixels to hide the confidential information [18–23]. Although this method is a non-reversible method, Lu et al. improved it to become reversible in 2015 [24]. They found that while using LSB matching, there are seven cases of modifications that cannot be recovered successfully, resulting in the method being non-reversible. To fix this problem, Lu et al. used a mapping table, which instructs the corresponding modifying rules to make the LSB matching method become a reversible technique when they encounter the non-reversible seven cases. After this method was proposed, many investigators began to study how improvements could increase the efficiency of this method. Tseng et al.'s scheme is one of these methods, which proposes a single-pixel hiding method that effectively improves the quality of stego-images [25]. Lu et al.'s method uses two pixels as a pair for dual-image hiding. That is, four pixels are used to hide four secret bits in each hiding process. Tseng et al.'s method, on the other hand, uses only one pixel of both images at a time. In other words, only two pixels of the two images are used at a time to embed two secret bits. Hence, the number of pixel modifications is reduced.

This investigation found that the hiding performance of Tseng et al.'s scheme is determined by the frequency of the modification. If one can control the modification times, then the image quality is controllable. Hence, this study analyzes the hidden rules of Tseng et al.'s scheme. The proposed scheme calculates in advance the number of occurrences of all hidden rules and the amount of modification to re-encode the confidential information for reducing the image distortion. Consequently, the proposed method achieves the result of improving stego-image visual quality.

2. Literature Discussion

In 2006, Mielikainen proposed an LSB matching method to embed two secret bits into two pixels. In their scheme, only one pixel will be modified in the embedding process such that effectively reduce the image distortion. However, the scheme is non-reversible. In 2015, Lu et al. extended the LSB matching method to become a reversible hiding scheme using dual-image technique. In Lu et al.'s scheme, four secret bits are concealed into two pixel-pairs in two copy images, respectively. After that, Wang et al. enhanced Lu et al.'s scheme to reuse the second pixel of the pixel pair for concealing one more secret bit. Different from Lu et al. and Wang et al.'s scheme, Tseng et al. use one pixel instead of two pixels in the pixel pair to embed one secret bit. More details about the related works are shown below.

2.1. Least Significant Bit (LSB) Matching Method

The LSB matching method, which was proposed by Mielikainen in 2006, improved on the LSB replacement method by Chen et al. in 2004. The image quality of Chen et al.'s scheme is poor when the amount of confidential information increases. Therefore, Mielikainen proposed the LSB matching method to improve the image quality of Chen et al.'s scheme [22]. The hiding flowchart of LSB replacement is shown in Figure 1.

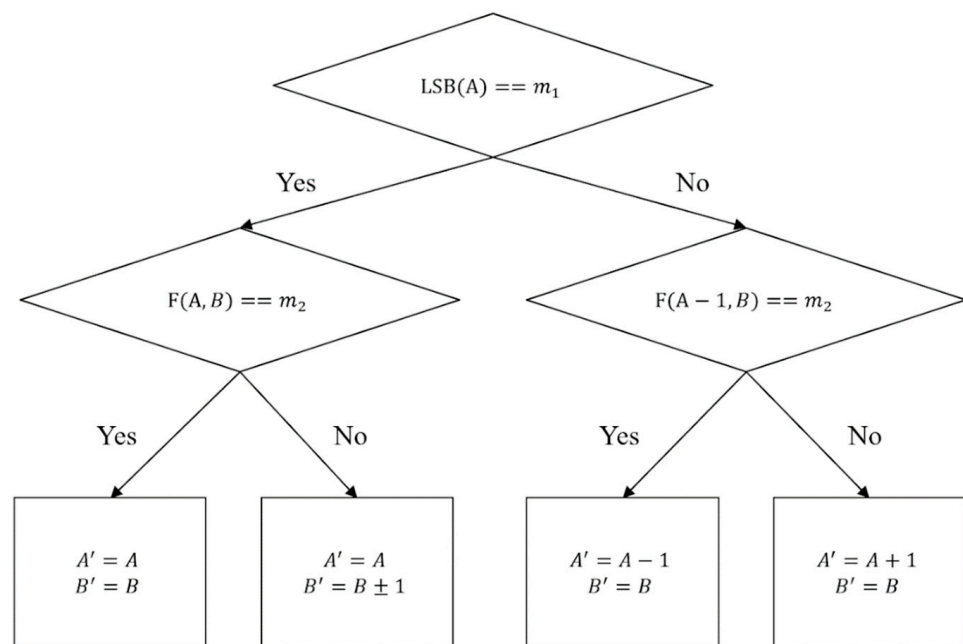


Figure 1. LSB matching hiding flowchart.

In their scheme, a cover image is divided into several 1×2 non-repetitive blocks, and A and B are represented as two pixels for each block. The confidential information to be hidden in each group is m_1 and m_2 . The scheme follows the tree flow diagram, as shown in Figure 1, to find the proper modify rule. The LSB of A is compared with m_1 , and then the value of F function is compared with m_2 to determine the final modify rule. The F function is shown as follows:

$$F(A, B) = LSB\left(\left\lfloor \frac{A}{2} \right\rfloor + B\right) \tag{1}$$

Four conditions of the final modify rule are shown, as follows:

- Case 1: When $LSB(A) = m_1$ and $F(A, B) = m_2$, the pixel pair A and B does not need modification.
- Case 2: When $LSB(A) = m_1$ and $F(A, B) \neq m_2$, the pixel A does not change, and $B = B + 1$ or $B = B - 1$.
- Case 3: When $LSB(A) \neq m_1$ and $F(A - 1, B) = m_2$, the pixel $A = A - 1$, and B does not change.
- Case 4: When $LSB(A) \neq m_1$ and $F(A - 1, B) \neq m_2$, the pixel $A = A + 1$, and B does not change.

After hiding each group of pixel pairs and confidential information in sequence, a camouflage image can be obtained.

When the receiver receives the camouflage image, the confidential information extraction process can be executed. The extraction formula is shown, as follows:

$$m_1 = LSB(A') \tag{2}$$

$$m_2 = LSB\left(\left\lfloor \frac{A'}{2} \right\rfloor + B'\right) \tag{3}$$

Finally, the hiding and extracting processes are done.

Let us assume the pixel pairs to be $A = 128, B = 130$ and the confidential information to be $s = (01)_2$. First, determine whether $LSB(128)$ is the same as the confidential message $m_1 = 0$. One can observe that $LSB(128)$ does equal 0. Therefore, the scheme uses the $LSB(128, 130)$ function to determine whether $LSB = LSB\left(\left\lfloor \frac{128}{2} \right\rfloor + 130\right)$ is the same as

$m_2 = 1$. According to the hiding flowchart, the result is that $LSB\left(\left\lfloor \frac{128}{2} \right\rfloor + 130\right) \neq 1$. Hence, the final modify rule is Case 2, where the pixel A does not change, and $B = B + 1$. Finally, these results are $A' = 128$ and $B' = 131$. The above numerical example shows the complete hiding process, and subsequently, when the recipient is restoring, the confidential information can be restored through Equations (2) and (3), $m_1 = LSB(128) = 0$, $m_2 = LSB\left(\left\lfloor \frac{128}{2} \right\rfloor + 131\right) = 1$.

2.2. Dual-Images Technique Based on the LSB Matching Method

Lu et al. proposed a dual-image LSB matching method in 2015 [24]. Lu et al. use a cover image to generate two copy images as the cover medium, instead of a single medium in LSB matching. Every two pixels in each copied image can hide two secret bits, or in other words, every two pixels can carry four secret bits in two copy images. This method can restore the original cover image after the extraction and recovery processes.

In the embedding procedure, the scheme copies the cover image into two identical images, then divides the original image into 1×2 non-repetitive blocks. The scheme sets the two pixels in the pixel group as A and B . Each group can contain four confidential messages $s = \{m_1 m_2 m_3 m_4\}$. The scheme uses the LSB matching method to hide m_1, m_2 into pixels A' and B' of the first camouflage image and m_3, m_4 are hidden in pixels A'' and B'' of the second camouflage image. After completing the concealment, it is necessary to confirm whether the camouflage image can be restored to the original image through the averaging method. The formula of the averaging method is as follows:

$$A^r = \left\lfloor \frac{A' + A''}{2} \right\rfloor, B^r = \left\lfloor \frac{B' + B''}{2} \right\rfloor \quad (4)$$

A^r and B^r represent the original value that was restored by the averaging method. When $A^r = A$ and $B^r = B$, it means that the pixel value of the camouflage image can be restored successfully without any modification. Otherwise, if $A^r \neq A$ or $B^r \neq B$, it means that the camouflage pixels are not able to be restored correctly. Therefore, the pixel values require a modification according to the seven modification rules designed by Lu et al. The seven modification rules are shown in Table 1 and the complete embedding flow chart is shown in Figure 2. In the table, TA' and TB' mean the temp stego-results of A and B in the first camouflage image. TA'' and TB'' mean the temp stego-results in the second camouflage image. After adjustment, the final camouflage pixels are modified to A', B', A'' and B'' .

Table 1. The seven Modification Rules designed by Lu et al.

Rule	Pixel Value Condition				Final Adjustment			
	TA'	TB'	TA''	TB''	A'	B'	A''	B''
1	0	0	-1	0	$A + 2$	$B + 1$	$A - 1$	$B + 1$
2	0	1	0	1	A	$B + 1$	A	$B - 1$
3	0	1	-1	0	$A + 2$	B	$A - 1$	B
4	-1	0	0	0	$A - 1$	B	$A + 2$	$B + 1$
5	-1	0	0	1	$A - 1$	B	$A + 2$	B
6	-1	0	-1	0	$A - 1$	$B + 2$	$A + 1$	$B - 1$
7	1	0	1	0	$A - 1$	$B - 1$	$A + 1$	$B + 2$

In the extraction procedure, the scheme uses the same formula as LSB matching methods, like Equations (2) and (3), to extract the secret information. The original image can be recovered by using the averaging method in Equation (4). Consider the original pixels $A = 37$ and $B = 33$ as an example. First, the scheme duplicates the image into two images of identical size. The pixel pairs are $(A_1, B_1) = (A_2, B_2) = (37, 33)$ and set the secret data to $s = (0000)_2$. According to the LSB matching method $LSB(A_1) = LSB(37) = 1$, and because $LSB(37) \neq m_1 = 0$, it is replaced by $37 - 1 = 36$. The scheme puts 36 and $B_1 = 33$

into F function to obtain $F(36, 33) = LSB(51) = 1$. The value of the F function is not equal to $m_2 = 0$, and the result is Case 4, which is $TA' = A_1 + 1$ and $TB' = B_1$.

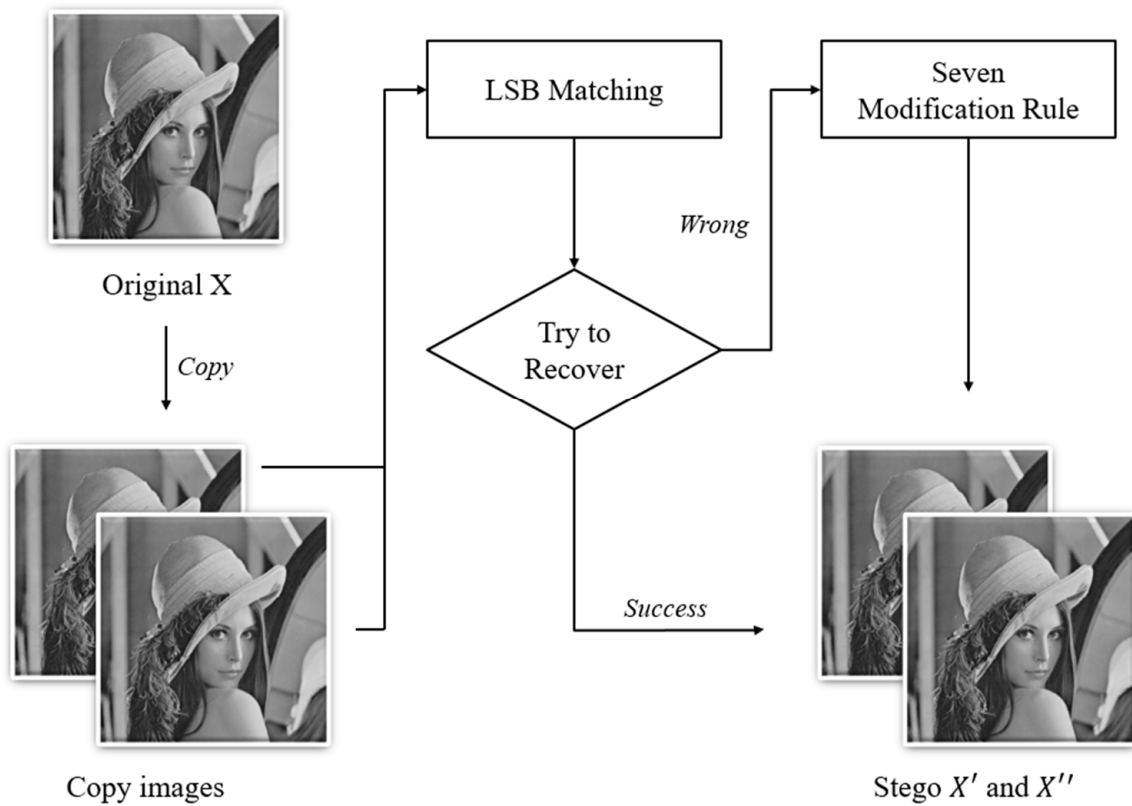


Figure 2. The flowchart of the dual-image LSB matching method proposed by Lu et al.

The pixel pair in the second image (A_2, B_2) hides the secret data $s = (00)_2$. After calculation, we obtain the same result, Case 4, which is $TA'' = A_2 + 1$ and $TB'' = B_2$. Second, the scheme checks whether the camouflage pixels can be recovered or not by referring to the seven modification rules. Here, we can see that Rule 7 of the seven modification rules confirms this, hence, the final camouflage pixels will be modified into $A' = 37 - 1 = 36$, $A'' = 37 - 1 = 36$, $B' = 33 - 1 = 32$, $A'' = 37 + 1 = 38$ and $B'' = 33 + 2 = 35$.

The extracting procedure can be implemented by using Equations (2) and (3). The scheme calculates the message $m_1 = LSB(36) = 0$ and $m_2 = LSB(\lfloor \frac{36}{2} \rfloor + 32) = LSB(50) = 0$ from the first pixel pair $(36, 32)$. The messages $m_3 = LSB(38) = 0$ and $m_4 = LSB(\lfloor \frac{38}{2} \rfloor + 35) = LSB(54) = 0$ are extracted from the second pixel pair $(38, 35)$. The complete confidential message is $s = (0000)_2$.

2.3. Improved Dual Image-Based RDH Using LSB Matching

In 2017, Wang et al. proposed an improved method of Lu et al.'s dual-image scheme [26]. The embedding process is roughly the same as that of Lu et al.'s scheme, but the difference is that after hiding two pixels, the scheme will then determine whether the second pixel can be used to conceal once again. Wang et al. proposed a new modified rule table to fix the recovery problem. The diagram of their scheme is shown in Figure 3. The formula to check whether the second pixel could be used once again is as follows:

$$|B' - B''| == 0 \tag{5}$$

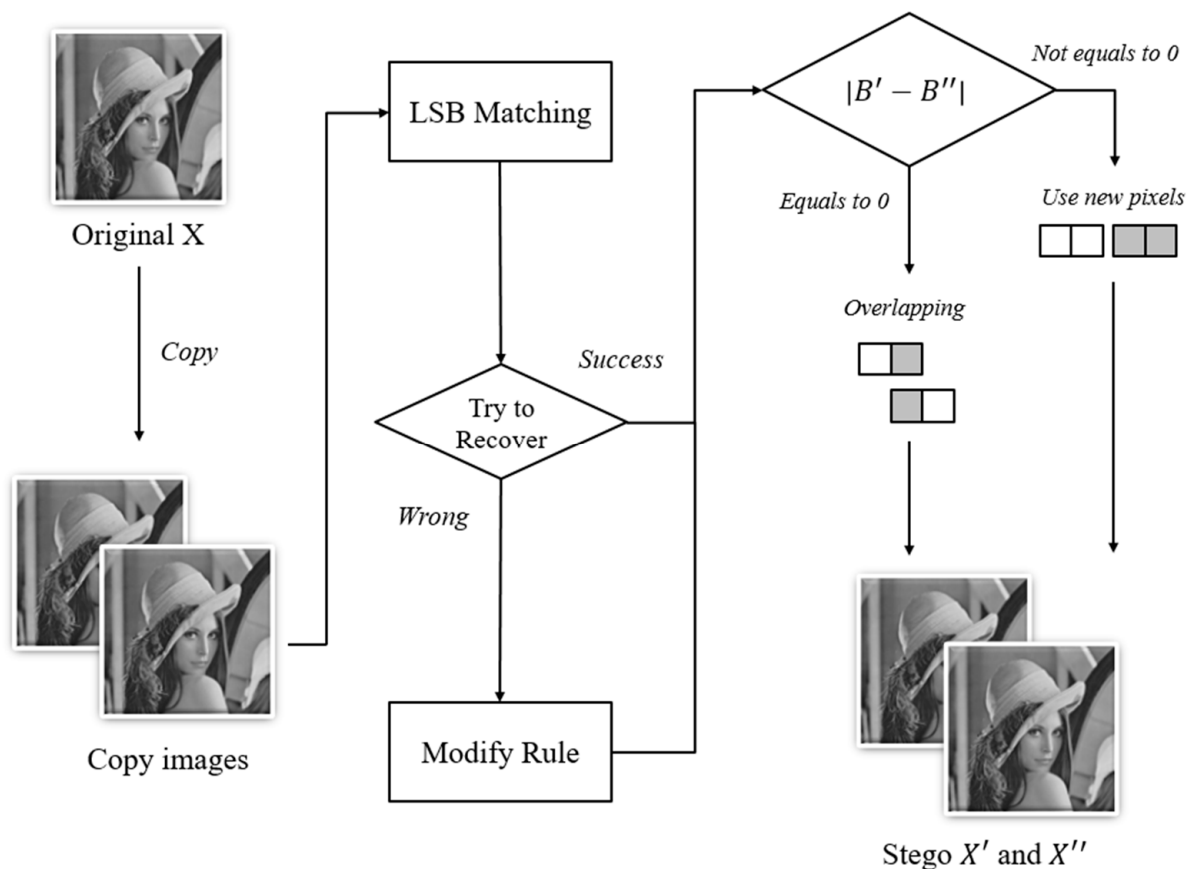


Figure 3. The flowchart of the dual-image LSB matching method by Wang et al.

In Equation (5), B' represents the second pixel of the first camouflage pixel pair, and B'' represents the second pixel of the second camouflage pixel pair. The equation means that if the second pixels in both first and the second camouflage images are the same, then the second pixel can be used once again.

The scheme takes two pixels as a pair and uses LSB matching to embed secret data. The detailed process is described as follows:

1. Duplicate the original image into two identical images.
2. Use LSB matching to embed secret data m_1m_2 into the first image to generate $\{TA', TB'\}$ and secret data m_3m_4 into the second image to generate $\{TA'', TB''\}$.
3. Look up Wang et al.'s modification rule table, as shown in Table 2, and modify the pixels that cannot be recovered properly. There are 11 cases in the modified rule table.
4. Use Equation (5) to check whether the second pixel can possibly be used to embed overlapping. If Equation (5) is satisfied, then the scheme uses the second pixel of the pixel pair as the first pixel to be hidden next time. Otherwise, if Equation (5) is not satisfied, the scheme skips the second pixel and finds a new pixel pair to embed the next occurrence of secret data.
5. Repeat Steps (2) to (4) until all secret data are embedded into two camouflage images.

The extracting procedure can be implemented by using Equation (6) to extract the first secret data and using Equation (7) to extract the second secret data. Similarly, the scheme uses Equations (8) and (9) to extract the third and fourth secret data. In the extracting procedure, the scheme needs to use Equation (5) to check whether the next pixel pair is overlapping or not. If the value of $|B' - B''|$ equals 0 or lower than 3, then the scheme uses the second pixel to perform the next extraction. Otherwise, the scheme uses the new pixel pair to extract secret data. Finally, Equation (10) is used to recover to the original pixel.

$$m_1 = LSB(A') \quad (6)$$

$$m_2 = LSB\left(\left\lfloor \frac{A'}{2} \right\rfloor + B'\right) \tag{7}$$

$$m_3 = LSB(A'') \tag{8}$$

$$m_4 = LSB\left(\left\lfloor \frac{A''}{2} \right\rfloor + B''\right) \tag{9}$$

$$A = \left\lfloor \frac{A' + A''}{2} \right\rfloor \tag{10}$$

Table 2. The Modify Rules Table designed by Wang et al.

Case	Pixel Value Condition				Final Adjustment			
	TA'	TB'	TA''	TB''	A'	B'	A''	B''
1	0	0	-1	0	$A + 2$	$B + 3$	$A - 1$	$B - 2$
2	0	1	0	1	A	$B + 3$	A	$B - 3$
3	0	1	-1	0	$A + 2$	$B - 1$	$A - 2$	$B + 2$
4	-1	0	0	0	$A - 1$	$B - 2$	$A + 2$	$B + 3$
5	-1	0	0	1	$A - 1$	$B + 2$	$A + 2$	$B - 2$
6	-1	0	-1	0	$A - 1$	$B + 4$	$A + 1$	$B - 3$
7	1	0	1	0	$A - 1$	$B - 3$	$A + 1$	$B + 4$
8	0	0	0	1	A	$B - 2$	A	$B + 3$
9	1	0	0	1	$A + 1$	$B - 2$	A	$B + 3$
10	0	1	1	0	A	$B + 3$	$A + 1$	$B - 2$
11	0	1	0	0	A	$B + 3$	A	$B - 2$

2.4. Tseng’s Dual Image-Based RDH on the Modified LSB Matching Method

In Lu et al.’s method, the seven modified rules are implemented to fix the cases, which are not recoverable to recover correctly [25]. In the modified rules, the greatest distortion made by each pixel is 2, which might be larger than the one produced by the regular LSB matching method. In 2019, Tseng et al. tackled this issue by changing the LSB matching embedding process. Instead of using two neighboring pixels, Tseng et al. used one pixel to make a pixel pair for hiding data by implementing the modified LSB matching. The camouflage pixels generated by modified LSB matching can be recovered correctly using the averaging method without any adjustment. Relying on these changes, Tseng et al.’s method can improve the image quality and achieve retrieval without using the rule table for modification. The embedding procedure is shown in Figure 4.

There are also four cases of modifications in the modified LSB matching, which are like the original LSB matching, with only Case 3 being different. This change is to ensure the recovery procedure can be executed successfully. Four conditions of the final modify rule by Tseng et al. are shown, as follows:

- Case 1: When $LSB(A) = m_1$ and $F(A, A) = m_2$, the pixel pair A' and A'' does not need modification.
- Case 2: When $LSB(A) = m_1$ and $F(A, A) \neq m_2$, the pixel $A' = A$, and $A'' = A + 1$.
- Case 3: When $LSB(A) \neq m_1$ and $F(A - 1, A) = m_2$, the pixel $A' = A + 1$, and $A'' = A - 1$.
- Case 4: When $LSB(A) \neq m_1$ and $F(A - 1, A) \neq m_2$, the pixel $A' = A + 1$, and $A'' = A$.

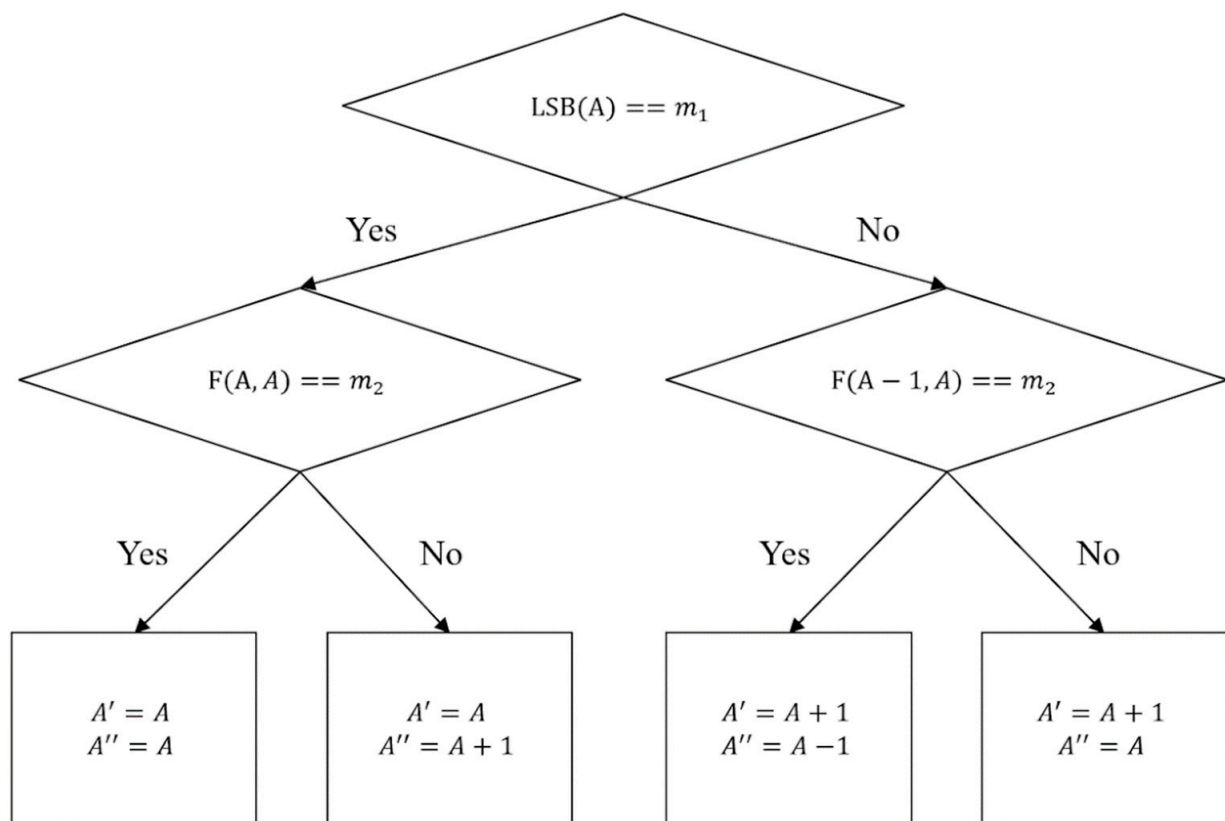


Figure 4. Dual-image modified LSB matching hiding flowchart by Tseng et al.

3. Research Methods

Tseng et al.'s scheme is efficient. In their method, the maximum modification is ± 1 according to the adjustment rules of LSB matching. The image quality of Tseng et al.'s scheme is very good.

In Tseng et al.'s scheme, each pixel depending on the secret message there might have several different cases. For an even pixel, its corresponding F function value might be 0 or 1. Each F function value has four different hiding cases 00, 01, 10, and 11. An odd pixel also has the same situation. Therefore, there are 2 (even or odd pixel) $\times 2$ (F value 0 or 1) $\times 4$ (secret messages 00, 01, 10, 11) = 16 different hiding cases.

If we could set up the most frequent case to have the lowest modified values, then the image distortion could be further reduced, such that the image quality could be improved.

Hence, the proposal tries to minimize the number of cases when the modified pixel values differ by 2. It is done by redefining the four maps above so that the worst case is used a minimal number of times. The new maps should be transferred to the receiver additionally to the stego-images. This study analysis and these statistics utilize the appearance rules of Tseng et al.'s scheme to adjust the modification rule table. The diagram of the proposed scheme is shown in Figure 5.

3.1. Preprocessing Procedure

By analyzing Tseng et al.'s scheme, we can find that a different parity of the pixel will cause different embedding results and will use different matching rules. In other words, the odd or even pixel value will affect its embedding orientation. For example, if A is an even number, then $F(A, A)$ is the same as $F(A + 1, A)$, and it has eight different possible results. On the other hand, if A is an odd number, the results of $F(A, A)$ are opposite of $F(A + 1, A)$, and it also has eight different possible results. For example, suppose that $A = 12$ is an even number, the value of $F(A, A) = F(12, 12) = \text{LSB}\left(\left\lfloor \frac{12}{2} \right\rfloor + 12\right) = 0$

is equal to $F(A + 1, A) = F(13, 12) = LSB\left(\left\lfloor \frac{13}{2} \right\rfloor + 12\right) = 0$. On the contrary, suppose that $A = 11$ is an odd number, the value of $F(A, A) = LSB\left(\left\lfloor \frac{11}{2} \right\rfloor + 11\right) = 0$ is different from $F(A + 1, A) = F(12, 11) = LSB\left(\left\lfloor \frac{12}{2} \right\rfloor + 11\right) = 1$. Therefore, we can ignore the modification of $F(A + 1, A)$ and just look at the part of $F(A, A)$. The analysis of $F(A, A)$ is shown in Table 3.

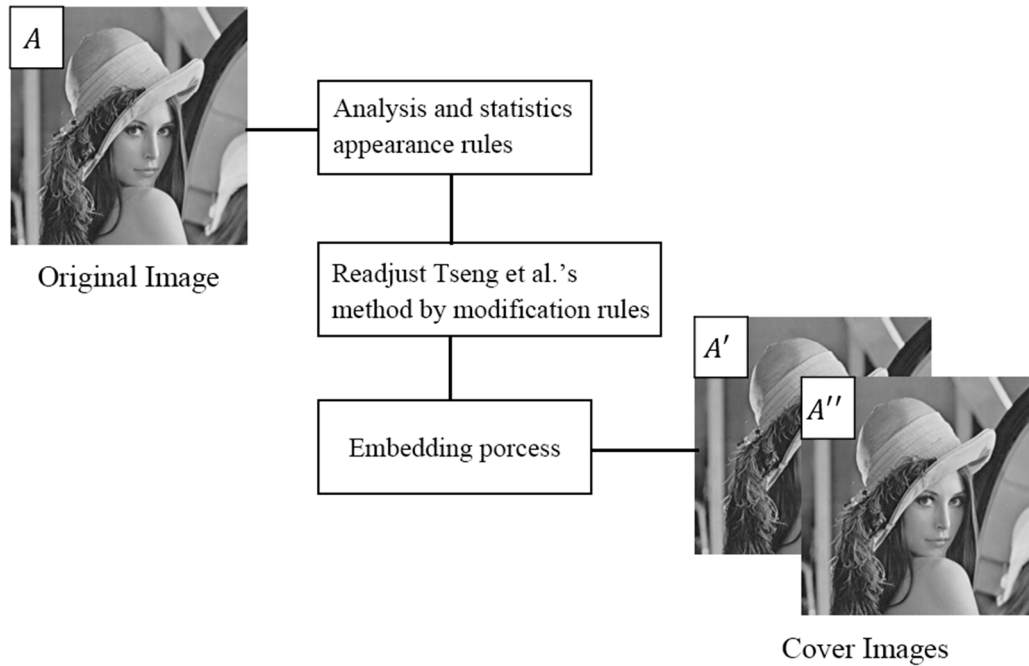


Figure 5. Diagram of the proposed method.

Table 3. Embedding Rules Table of the proposed scheme.

A	$LSB(A)$	$F(A, A)$	m_1	m_2	A'	A''	Distortion(δ)	Ordering(ρ)
Even	0	0	0	0	0	0	0	0
			0	1	0	+1	1	1
			1	0	+1	0	1	2
			1	1	-1	+1	2	3
		1	0	0	0	+1	1	1
			0	1	0	0	0	0
			1	0	-1	+1	2	3
			1	1	+1	0	1	2
Odd	1	1	0	1	-1	+1	2	3
			1	0	0	+1	1	2
			1	1	0	0	0	0
			0	0	-1	+1	2	3
		0	0	1	+1	0	1	1
			1	0	0	0	0	0
			1	0	0	0	0	0
			1	1	0	+1	1	2

In the first part, if A is an even number, then there are two different cases of $F(A, A)$ for embedding the secret message, where $F(A, A) = 0$ or $F(A, A) = 1$. Furthermore, for each case of $F(A, A)$ there are four different embedding situations with m_1 and m_2 . Therefore, there are eight different cases applicable to an even number. For example, suppose that $A = 12$, then $LSB(A) = LSB(12) = 0$ and the value of $F(A, A) = F(12, 12) = LSB\left(\left\lfloor \frac{12}{2} \right\rfloor + 12\right) = 0$. If $m_1 = 1$ and $m_2 = 1$, then $A' = A + 1 = 13$

and $A'' = A - 1 = 11$. The image distortion made by this case is $\delta = (A' - A)^2 + (A'' - A)^2 = (13 - 12)^2 + (11 - 12)^2 = 2$. There are also eight different cases for an odd number. For example, suppose that $A = 9$, then $LSB(A) = LSB(9) = 1$ and the value of $F(A, A) = F(9, 9) = LSB(\lfloor \frac{9}{2} \rfloor + 9) = 1$. If $m_1 = 1$ and $m_2 = 0$, then $A' = A = 9$ and $A'' = A + 1 = 10$. The image distortion made by this case is $\delta = (A' - A)^2 + (A'' - A)^2 = (9 - 9)^2 + (9 - 10)^2 = 1$.

For the even number with $LSB(A)$ and $F(A, A) = 0$, the distortions for the message bits (m_1, m_2) with $(0,0)$, $(0,1)$, $(1,0)$, and $(1,1)$ are 0, 1, 1, and 2, respectively. The scheme ranks the four cases according to their corresponding distortion value. The column "Ordering (ρ)" in Table 3 shows the ordering results. The maximum distortion $\delta = 2$ is made by the cases with $\rho = 3$. In other words, if the occurrence frequency of the cases with $\rho = 3$ is large then the image quality becomes worse.

Before the embedding procedure, the proposed scheme analyzes the occurrence frequency of every combination between the cover image and the secret message, for generating a re-encoding table. In the analysis processing, a cover pixel A is duplicated to generate two temp pixels for concealing two message bits m_1 and m_2 . In Table 4, the symbol γ is the frequency of the combination, δ is the distortion made by the modification, ρ is the original order sorting by δ , and θ is the total distortion computed by $\theta = \gamma \times \delta$. The scheme re-orders the combination according to γ in a decreasing order to get the new order $\hat{\rho}$ of each combination.

Table 4. The Re-encoding Table of the proposed scheme.

A	LSB(A)	F(A, A)	m ₁	m ₂	t	γ	δ	ρ	ρ̂
Even	0	0	0	0	0	γ ₀ ⁰ (0)	δ ₀ ⁰ (0)	ρ ₀ ⁰ (0)	ρ̂ ₀ ⁰ (0)
			0	1	1	γ ₀ ⁰ (1)	δ ₀ ⁰ (1)	ρ ₀ ⁰ (1)	ρ̂ ₀ ⁰ (1)
			1	0	2	γ ₀ ⁰ (2)	δ ₀ ⁰ (2)	ρ ₀ ⁰ (2)	ρ̂ ₀ ⁰ (2)
			1	1	3	γ ₀ ⁰ (3)	δ ₀ ⁰ (3)	ρ ₀ ⁰ (3)	ρ̂ ₀ ⁰ (3)
		1	0	0	0	γ ₁ ⁰ (0)	δ ₁ ⁰ (0)	ρ ₁ ⁰ (0)	ρ̂ ₁ ⁰ (0)
			0	1	1	γ ₁ ⁰ (1)	δ ₁ ⁰ (1)	ρ ₁ ⁰ (1)	ρ̂ ₁ ⁰ (1)
			1	0	2	γ ₁ ⁰ (2)	δ ₁ ⁰ (2)	ρ ₁ ⁰ (2)	ρ̂ ₁ ⁰ (2)
			1	1	3	γ ₁ ⁰ (3)	δ ₁ ⁰ (3)	ρ ₁ ⁰ (3)	ρ̂ ₁ ⁰ (3)
			⋮	⋮	⋮	⋮	⋮	⋮	⋮
			⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	γ _{F(A,A)} ^{LSB(A)} (t)	δ _{F(A,A)} ^{LSB(A)} (t)	ρ _{F(A,A)} ^{LSB(A)} (t)	ρ̂ _{F(A,A)} ^{LSB(A)} (t)	

In Table 4, $\gamma_{F(A,A)}^{LSB(A)}(t)$ means the frequency of the combination with $LSB(A)$ and $F(A, A)$ in the t th case, where $0 \leq t \leq 3$. For example, $\gamma_0^0(3)$ is the frequency for an even number, which is $LSB(A) = 0$ and $F(A, A) = 0$ in the case where $t = 3$, which results in $m_1 = 1$ and $m_2 = 1$. $\delta_{F(A,A)}^{LSB(A)}(t)$ is the distortion computed by $(A' - A)^2 + (A'' - A)^2$ with $LSB(A)$ and $F(A, A)$ in the t th case. $\rho_{F(A,A)}^{LSB(A)}(t)$ is the ranking of the combination that is sorted by $\delta_{F(A,A)}^{LSB(A)}(t)$ in decreasing order. The scheme re-ranks the combination to get the new order $\hat{\rho}_{F(A,A)}^{LSB(A)}(t)$ by sorting $\gamma_{F(A,A)}^{LSB(A)}(t)$ in decreasing order.

An example is shown in Table 5. In the table, the occurrence frequency of the even pixel that conceals $(m_1, m_2) = (1, 0)$ is $\gamma_{F(A,A)=0}^{LSB(A)=0}(2) = 135$. The distortion made by the modification rule, which is shown in Table 3, is $\delta_{F(A,A)=0}^{LSB(A)=0}(2) = (+1)^2 + (0)^2 = 1$. There are 135 pixels, which have the same attributes. Hence, the total number of the distortion is $\theta_{F(A,A)=0}^{LSB(A)=0}(2) = \gamma_{F(A,A)=0}^{LSB(A)=0}(2) \times \delta_{F(A,A)=0}^{LSB(A)=0}(2) = 135 \times 1 = 135$. Because $\gamma_{F(A,A)=0}^{LSB(A)=0}(2) = 135 \geq \gamma_{F(A,A)=0}^{LSB(A)=0}(0) = 50 \geq \gamma_{F(A,A)=0}^{LSB(A)=0}(3) = 45 \geq \gamma_{F(A,A)=0}^{LSB(A)=0}(1) = 40$, the order of the

combination, with $LSB(A) = 0$ and $F(A, A) = 0$, becomes $\hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(t) = \{1, 3, 0, 2\}$. The case $t = 2$ is the highest frequency case, hence, the new order of the combination is the smallest value, where $\hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(2) = 0$. The first case is the second frequency case, so the new order is $\hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(0) = 1$.

Table 5. A Re-encoding Table example.

A	LSB(A)	F(A, A)	t	m ₁	m ₂	γ	δ	ρ	θ	δ̂	ρ̂	θ̂	
Even	0	0	0	0	0	50	0	0	0	1	1	50	
			1	0	1	40	1	1	40	2	3	80	
			2	1	0	135	1	2	135	0	0	0	
			3	1	1	45	2	3	90	1	2	45	
			0	0	0	120	1	1	120	0	0	0	
		1	1	0	1	50	0	0	0	2	3	100	
			2	1	0	60	2	3	120	1	2	60	
			3	1	1	80	1	2	80	1	1	80	
			0	0	0	110	1	1	110	1	1	110	
			1	0	1	130	2	3	260	0	0	0	
Odd	1	1	2	1	0	10	1	2	10	2	3	20	
			3	1	1	50	0	0	0	1	2	50	
			0	0	0	30	2	3	60	1	2	30	
		0	1	0	1	20	1	1	20	2	3	40	
			2	1	0	100	0	0	0	0	0	0	
			3	1	1	50	1	2	50	1	1	50	
			Total distortion									1095	715

The mapping of ρ and $\hat{\rho}$ of the re-encoding table is used in the embedding and extraction processes.

3.2. Embedding Process

The proposed scheme uses one cover pixel A to embed two message bits m_1, m_2 in each embedding procedure. To reduce the total amount of distortion, the highest frequency combination is assigned the rule, which has the least distortion. Hence, the scheme modifies the pixel by using the altered rules in Table 6. Let $LA'_{F(A, A)}^{LSB(A)}(\hat{\rho})$ be the first rule used to modify the first camouflage pixel A' , and $LA''_{F(A, A)}^{LSB(A)}(\hat{\rho})$ be the second rule to modify the second camouflage pixel A'' . The symbol $\hat{\rho}$ is the new order of the combination.

The scheme uses A to compute $LSB(A)$ and $F(A, A)$ along with m_1 and m_2 to map the re-encoding table for obtaining the new order $\hat{\rho}_{F(A, A)}^{LSB(A)}(t)$. The alter rules are $LA'_{F(A, A)}^{LSB(A)}(\varepsilon)$ and $LA''_{F(A, A)}^{LSB(A)}(\varepsilon)$, where $\varepsilon = \hat{\rho}_{F(A, A)}^{LSB(A)}(t)$. For example, if we assume that the pixel is even, then $A = 14$, $LSB(A) = 0$, and $F(A, A) = 1$. The alter rules for ε being equal to 0, 1, 2, and 3 are $(LA'_{F(A, A)=1}^{LSB(A)=0}(\varepsilon), LA''_{F(A, A)=1}^{LSB(A)=0}(\varepsilon)) = (+0, +0), (+0, +1), (+1, +0),$ and $(-1, +1)$, respectively.

For the other example, let us assume that an odd pixel is $A = 15$, $LSB(A) = 1$ and $F(A, A) = 0$. The alter rules then are $(+0, +0), (+1, +0), (+0, +1),$ and $(-1, +1)$, respectively.

Following the same example shown above, the new order of the even pixel that conceals $(m_1, m_2) = (1, 0)$ is $\hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(2) = 0$. Because $\varepsilon = \hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(2) = 0$ the altered rule is $(LA'_{F(A, A)=0}^{LSB(A)=0}(0), LA''_{F(A, A)=0}^{LSB(A)=0}(0)) = (+0, +0)$. The new distortion is $\hat{\delta}_{F(A, A)=0}^{LSB(A)=0}(2) = (0)^2 + (0)^2 = 0$. The total number of distortions becomes $\hat{\theta}_{F(A, A)=0}^{LSB(A)=0}(2) = \gamma_{F(A, A)=0}^{LSB(A)=0}(2) \times \delta_{F(A, A)=0}^{LSB(A)=0}(2) = 135 \times 0 = 0$. The image distortion is reduced from 135 to 0. The total amount of the distortion, using the original modification rules table, which is

shown in Table 5, is 1095. On the other hand, the total amount, using the new alter rules, is 715. Hence, the proposed scheme indeed effectively reduces image distortion.

Table 6. The final Re-encoding Table.

$LSB(A)$	$F(A, A)$	m_1	m_2	t	$\hat{\rho}$	ρ	LA'	LA''
0	0	0	0	0	1	0	0	0
		0	1	1	3	1	0	+1
		1	0	2	0	2	+1	0
		1	1	3	2	3	-1	+1
		0	0	0	0	1	0	+1
	1	0	1	1	3	0	0	0
		1	0	2	2	3	-1	+1
		1	1	3	1	2	+1	0
		0	0	0	1	1	+1	0
		0	1	1	0	3	3	-1
1	1	1	0	2	3	2	0	+1
		1	1	3	2	0	0	0
		0	0	0	2	3	-1	+1
	0	0	1	1	3	1	+1	0
		1	0	2	0	0	0	0
		1	1	3	1	2	0	+1

The detailed process of the proposed scheme is described, as follows:

1. Preprocessing:
 - A. Set X to be the original image and s to be the secret message.
 - B. Use two secret bits m_1 and m_2 of s and the corresponding pixel A of X to count the occurrence frequency.
 - C. Compute $LSB(A)$ and $F(A, A)$ and $t = m_1 \times 2 + m_2$.
 - D. Calculate the frequency by $\gamma_{F(A, A)}^{LSB(A)}(t) = \gamma_{F(A, A)}^{LSB(A)}(t) + 1$.
 - E. Map the embedding rule table, which is shown in Table 4, to find the corresponding modification rule.
 - F. Calculate the distortion $\delta_{F(A, A)}^{LSB(A)}(t) = (A - A')^2 + (A - A'')^2$.
 - G. Repeat (B)–(F) until all pixels have been processed.
 - H. Rank the combinations by $\delta_{F(A, A)}^{LSB(A)}(t)$ in increasing order to obtain $\rho_{F(A, A)}^{LSB(A)}(t)$.
 - I. Rank the combinations by $\gamma_{F(A, A)}^{LSB(A)}(t)$ in decreasing order to obtain $\hat{\rho}_{F(A, A)}^{LSB(A)}(t)$.
2. Embedding Process:
 - A. Rescan the image X and re-start from the first bit of s .
 - B. Use two secret bits m_1 and m_2 of s and the corresponding pixel A of X to compute $LSB(A)$, $F(A, A)$ and $t = m_1 \times 2 + m_2$.
 - C. Use the values $LSB(A)$, $F(A, A)$ and t to find the corresponding order $\hat{\rho}_{F(A, A)}^{LSB(A)}(t)$.
 - D. Set $\varepsilon = \hat{\rho}_{F(A, A)}^{LSB(A)}(t)$.
 - E. Find the rule $(LA'_{F(A, A)}^{LSB(A)}(\varepsilon), LA''_{F(A, A)}^{LSB(A)}(\varepsilon))$ from Table 6 to compute A' and A'' .
 - F. Repeat the steps (B)–(E) until all messages are embedded into the image.

Figure 6 shows an embedding example. The original image is $X = \{44, 45, 37, \dots, 5\}$. The first pixel is 44. Suppose that the secret data is $s = (10)_2$. The scheme calculates the LSB function and F function to get $LSB(44) = 0$ and $F(44, 44) = LSB(\lfloor \frac{44}{2} \rfloor + 44) = 0$. Suppose that the final re-encoding table is shown in Table 6. The new code of the combination with $LSB(A) = 0$, and $F(A, A) = 0$ and $t = m_1 \times 2 + m_2 = 2$ is $\varepsilon = \hat{\rho}_{F(A, A)=0}^{LSB(A)=0}(2) = 0$. The

altered rules of $\varepsilon = 0$ are $(LA'_{F(A,A)=0}^{LSB(A)=0}(0), LA''_{F(A,A)=0}^{LSB(A)=0}(0)) = (+0, +0)$. Therefore, the stego-pixels are $A' = 44 + 0 = 44$ and $A'' = 44 + 0 = 44$.

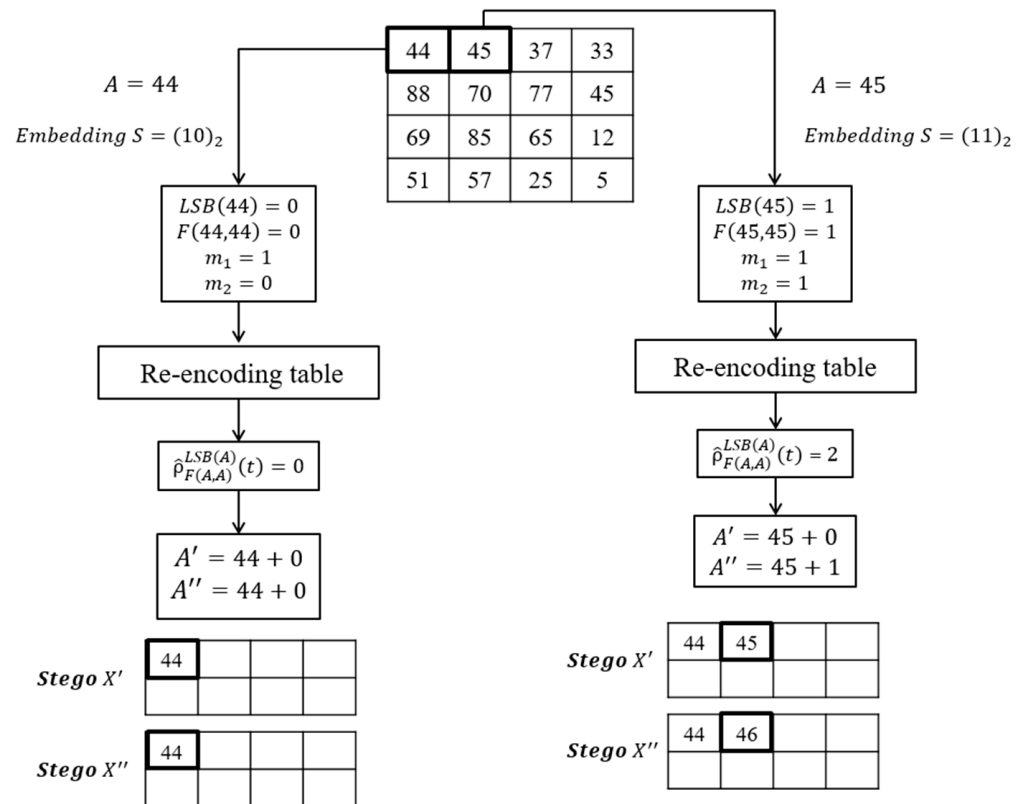


Figure 6. An embedding example.

The next pixel is 45, if the confidential message is $s = (11)_2$. The function values are $LSB(45) = 1$, and $F(45, 45) = 1$. The new code of the combination with $LSB(A) = 1$, $F(A, A) = 1$ and $t = m_1 \times 2 + m_2 = 3$ is $\hat{p}_{F(A,A)=1}^{LSB(A)=1}(3) = 2$. The alter rule of $\varepsilon = \hat{p}_{F(A,A)=1}^{LSB(A)=1}(3) = 2$ is $(LA'_{F(A,A)=1}^{LSB(A)=1}(2), LA''_{F(A,A)=1}^{LSB(A)=1}(2)) = (+0, +1)$. The stego-pixels are $A' = 45 + 0 = 45$ and $A'' = 45 + 1 = 46$.

The two camouflage images along with the re-encoding table are sent to the receiver for further extracting and recovering.

3.3. Information Extraction and Image Restoration Phase

In this phase, the receiver starts the procedure after having received two camouflage images and the re-encoding table. This method for information extraction is like Tseng et al.'s scheme. The original pixel value A is restored by calculating the floor average of two camouflage pixels A' and A'' .

$$A = \left\lfloor \frac{A' + A''}{2} \right\rfloor \tag{11}$$

The information extraction procedure can be implemented after recovering A because the scheme needs the original pixel value to do the calculation for some cases.

First, the scheme extracts the temp messages by using Equations (12) and (13).

$$\hat{m}_1 = LSB(A') \tag{12}$$

$$\hat{m}_2 = \begin{cases} \text{LSB}\left(\left\lfloor \frac{A}{2} \right\rfloor + A''\right), & \text{if } |A' - A''| = 2, \\ \text{LSB}\left(\left\lfloor \frac{A'}{2} \right\rfloor + A''\right), & \text{otherwise.} \end{cases} \tag{13}$$

The messages obtained from Equations (12) and (13) are not the original messages. Hence, the scheme uses the symbols \hat{m}_1 and \hat{m}_2 to represent the temp messages. The formula for extracting \hat{m}_1 is obtained by calculating the LSB of the pixel value of the first camouflage image. There are two situations for extracting \hat{m}_2 . If the distance between two camouflage pixels A' and A'' is equal to 2, then the embedding rule used in the pixel is ($A' = A - 1$ and $A'' = A + 1$). The extracted message might be wrong when the extraction equation is equal to $\text{LSB}(\lfloor A'/2 \rfloor + A'')$. Hence, the equation is changed to $\text{LSB}(\lfloor A/2 \rfloor + A'')$.

The order of the combination is recovered by the following equations.

$$\rho = \hat{m}_1 \times 2 + \hat{m}_2 \tag{14}$$

The scheme uses ρ to map the corresponding new order $\hat{\rho}$ from the re-encoding table. The corresponding messages are extracted by mapping $\hat{\rho}$ to m_1 and m_2 . For example, suppose that $A = 44$, $m_1 = 0$, and $m_2 = 1$. The function values are $\text{LSB}(44) = 0$ and $F(44, 44) = 0$. The new code of the combination with $\text{LSB}(44) = 0$ and $F(44, 44) = 0$ and $t = m_1 \times 2 + m_2 = 1$ is $\hat{\rho}_{F(A,A)=0}^{\text{LSB}(A)=0}(1) = 3$. The alter rule of $\varepsilon = \hat{\rho}_{F(A,A)=0}^{\text{LSB}(A)=0}(1) = 3$ is $(LA'_{F(A,A)=0}^{\text{LSB}(A)=0}(3), LA''_{F(A,A)=0}^{\text{LSB}(A)=0}(3)) = (-1, +1)$. The stego-pixels are $A' = 44 - 1 = 43$ and $A'' = 44 + 1 = 45$.

In the extraction phase, the original pixel is recovered by $A = \lfloor (A' + A'')/2 \rfloor = \lfloor (43 + 45)/2 \rfloor = 44$. The first temp secret bit is computed by $\hat{m}_1 = \text{LSB}(A') = \text{LSB}(43) = 1$. Because $|A' - A''| = |43 - 45| = 2$, the second bit is calculated by $\hat{m}_2 = \text{LSB}(\lfloor A/2 \rfloor + A'') = \text{LSB}(\lfloor 44/2 \rfloor + 45) = 1$. The order of the combination is $\rho = \hat{m}_1 \times 2 + \hat{m}_2 = 1 \times 2 + 1 = 3$. The scheme uses $\text{LSB}(A) = 0$ and $F(A, A) = 0$ and $\rho = 3$ to map the corresponding new order $\hat{\rho}$ from the re-encoding table, which is shown in Table 6. The corresponding messages are extracted by mapping $\hat{\rho}$ to its corresponding message $m_1 = 0$ and $m_2 = 1$. The diagram of the mapping is shown in Figure 7.

$\text{LSB}(A)$	$F(A, A)$	m_1	m_2	t	$\hat{\rho}$	ρ	LA'	LA''	
0	0	0	0	0	1	0	0	0	
		0	1	1	3	1	0	+1	
		1	0	2	0	2	+1	0	
		1	1	3	0	3	-1	+1	
	1	0	0	0	0	0	1	0	+1
			0	1	1	3	0	0	0
		1	1	0	2	2	3	-1	+1
			1	1	3	1	2	+1	0

Figure 7. The mapping of $\rho = 3$ to its corresponding $\hat{\rho}$ and messages m_1 and m_2 .

Similarly, let us take Figure 6 as an example. The first pixel is recovered by $A = \lfloor (44 + 44)/2 \rfloor = 44$. The temp messages are $\hat{m}_1 = \text{LSB}(44) = 0$ and $\hat{m}_2 = \text{LSB}(\lfloor 44/2 \rfloor + 44) = 0$. The order value is $\rho = \hat{m}_1 \times 2 + \hat{m}_2 = 0$. The corresponding new order $\hat{\rho}$ of the combination with $\text{LSB}(44) = 0$ and $F(A, A) = 0$ and $\rho = 0$ is $\hat{\rho}_{F(A,A)=0}^{\text{LSB}(A)=0}(2) = 0$, where $t = 2$.

The mapping messages are $m_1 = 1$ and $m_2 = 0$. The diagram of the mapping is shown in Figure 8.

$LSB(A)$	$F(A, A)$	m_1	m_2	t	$\hat{\rho}$	ρ	LA'	LA''
0	0	0	0	0	1	0	0	0
		0	1	1	3	1	0	+1
		1	0	2	0	2	+1	0
		1	1	3	2	3	-1	+1
	0	0	0	0	0	1	0	+1

Figure 8. The mapping of $\rho = 0$ to its messages $m_1 = 1$ and $m_2 = 0$.

The second pixel is $A = \lfloor \frac{45+46}{2} \rfloor = 45$. The temp messages are $\hat{m}_1 = LSB(45) = 1$ and $\hat{m}_2 = LSB(\lfloor 45/2 \rfloor + 46) = 0$. The order value is $\rho = 1 \times 2 + 0 = 2$. The corresponding new order $\hat{\rho}$ of the combination with $LSB(45) = 1$ and $F(45,45) = 1$ and $\rho = 2$ is $\hat{\rho}_{F(A,A)=1}^{LSB(A)=1}(t) = 2$, where $t = 3$. The mapping messages are $m_1 = 1$ and $m_2 = 1$. The final confidential message is $S = (1011)_2$. The diagram of the embedding example is shown in Figure 9.

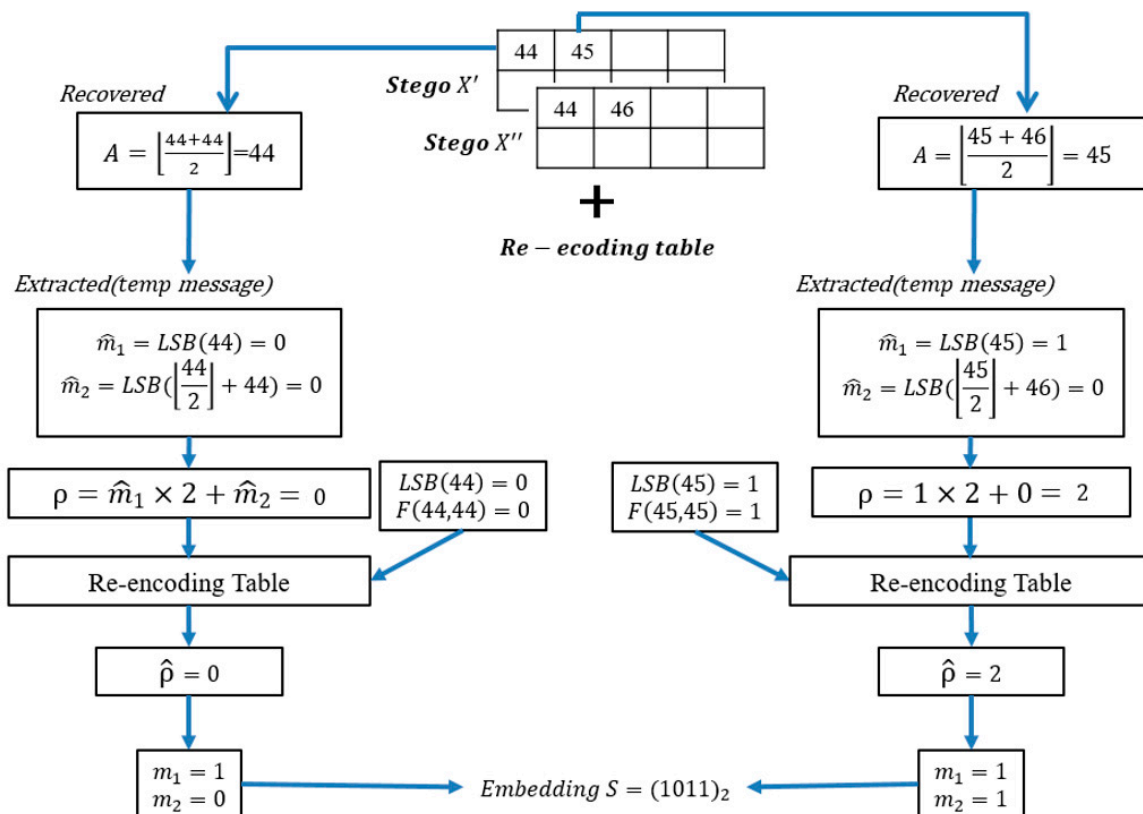


Figure 9. The extraction example of Figure 6.

3.4. Overflow and Underflow Problem

The method proposed in this study is an improvement on the method suggested by Tseng et al.'s scheme. Therefore, the same overflow and underflow problems will exist. To solve this problem and avoid these issues, we could apply the same rules as the method

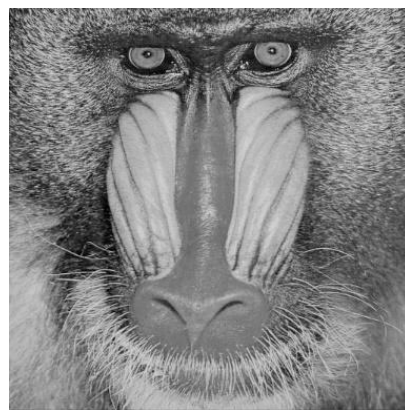
proposed by Tseng et al. If the original pixel value is equal to 0 or 255, then the pixel is non-embeddable and cannot be used to conceal the message. For the non-embeddable pixel, the value will remain unchanged. In the extraction process, if both camouflage pixels are equal to 0 or 255, then it means there is no secret data hidden in it. Even if only one stego-pixel value is equal to 0 or 255 it is evident that it still has the secret message concealed in it.

4. Experimental Results and Discussions

This research employed Matlab (version R2016b) as the test environment, and used six grayscale images (512×512 in size) to conduct experiments in order to verify whether the research method can effectively improve the image quality. The following figures show the six grayscale images used in the experiment. The test images are Lena, Mandrill, Pepper, Airplane, Lake, and Tiffany. The images are shown in Figure 10.



(a) Lena



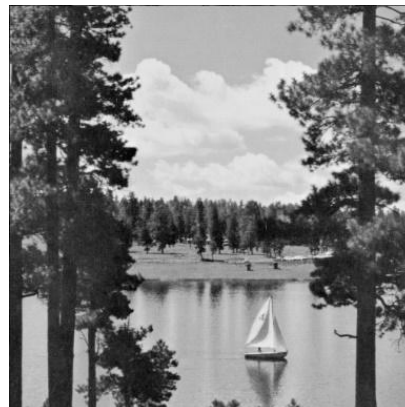
(b) Mandrill



(c) Pepper



(d) Airplane



(e) Lake



(f) Tiffany

Figure 10. The six test images (a) Lena (b) Mandrill (c) Pepper (d) Airplane (e) Lake (f) Tiffany each of them has different characteristics.

In the experiment, the Peak Signal-to-Noise Ratio (PSNR) is used to quantify the image quality. PSNR is usually expressed as a logarithmic quantity using the decibel (dB) scale. The following is the definition of PSNR:

$$PSNR = 10 \times \left(\frac{255^2}{MSE} \right) (dB) \quad (15)$$

The MSE of the equation is the mean square error, which represents the square root of the difference between the original image and the camouflage image. Therefore, the smaller the MSE value, the better the calculated image quality. The MSE formula is as follows:

$$MSE = \frac{1}{h \times w} \sum_{i=1}^h \sum_{j=1}^w (x_{i,j} - x'_{i,j})^2 \quad (16)$$

h and w , respectively, represent the length and width of the image, $x_{i,j}$ represents the pixels of the original image, and $x'_{i,j}$ represents the pixels of the camouflage image. Dual-image technology is implemented in this paper. Hence, we used the average of the two camouflage-image PSNR values in our comparison with other methods.

The hiding payload is computed by:

$$\text{bpp} = \frac{TB}{2 \times h \times w}. \quad (17)$$

where TB is the total number of secret message bits, which are embedded into the cover image (and “bpp” means bits per pixel). Because the proposed scheme is a dual-image based scheme, the total number of pixels is $2 \times h \times w$.

This study compares the proposed scheme with Lee et al.’s scheme, schemes Lee2009 and Lee2013 [6,7], Qin and Chang et al.’s scheme [3], the center folding scheme (CenterFolding) proposed by Lu et al. [9], LSB-M proposed by Lu et al. [24], and LSB-MA proposed by Tseng et al. [25]. The proposed scheme is indicated with LSB-MA-ordering. Figures 11–13 show the experimental results.

In the first experiment, the scheme randomly generates the secret message and conceals it into the test image. Figure 11 shows the results of concealing the random bits into Lena. The hiding payloads of Chang2013 and Center Folding are higher than that of the others, however, the PSNR values of Chang2013 and CenterFolding are worse than that of the others. The LSB matching based schemes can achieve higher image quality. Among them, the hiding payload of Lee2009 is the least. The image quality of LSB-MA-ordering is the highest.

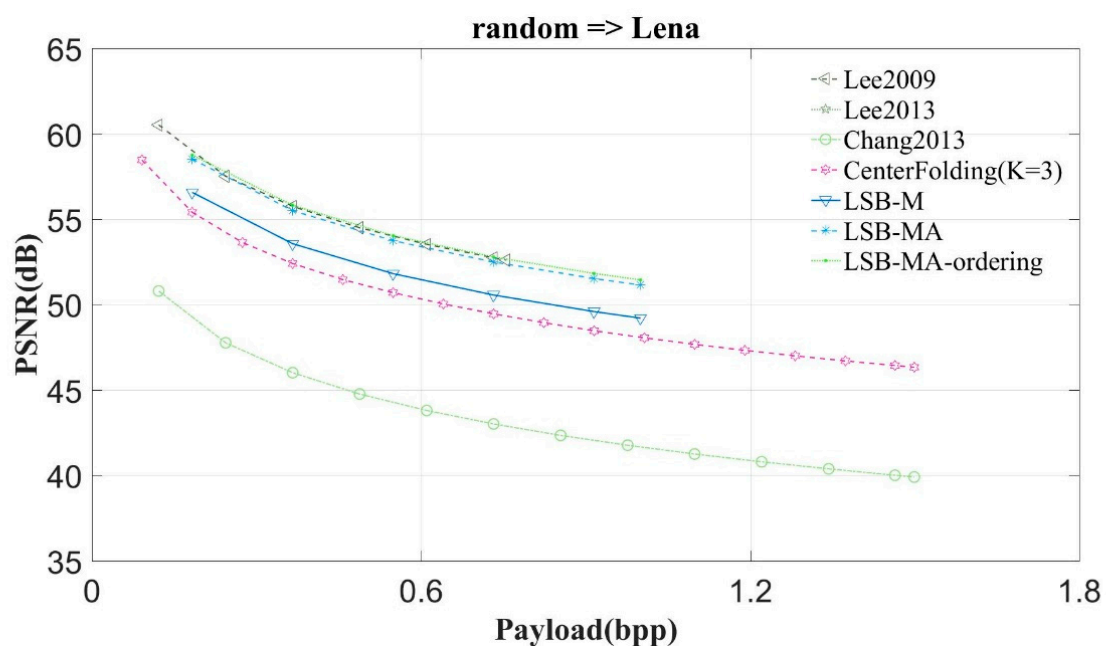


Figure 11. The experimental results of Lena.

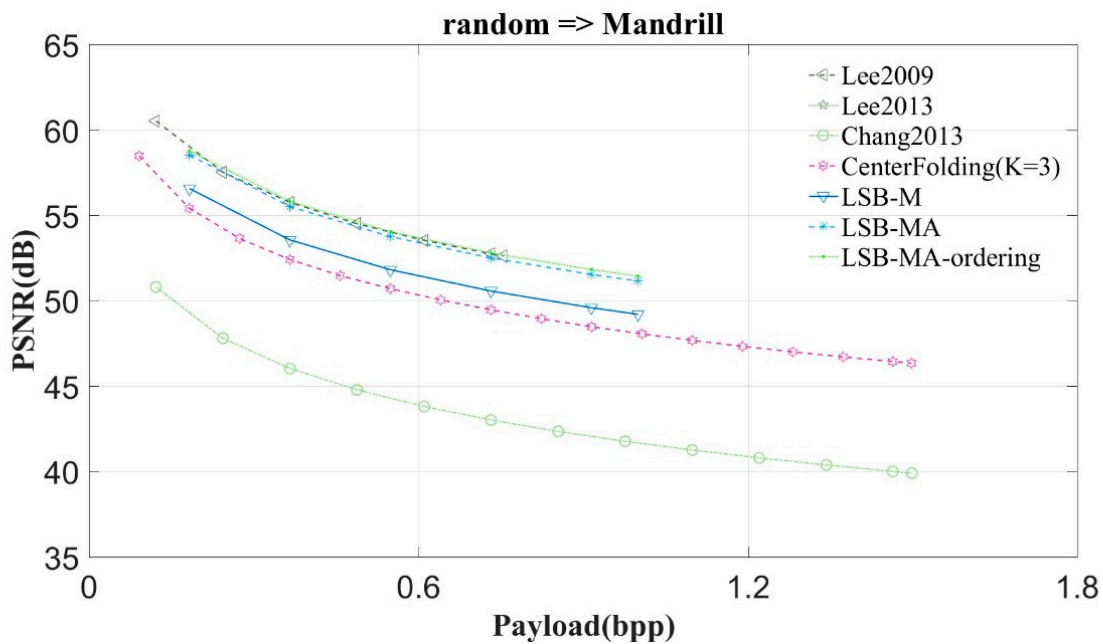


Figure 12. The experimental results of Mandrill.

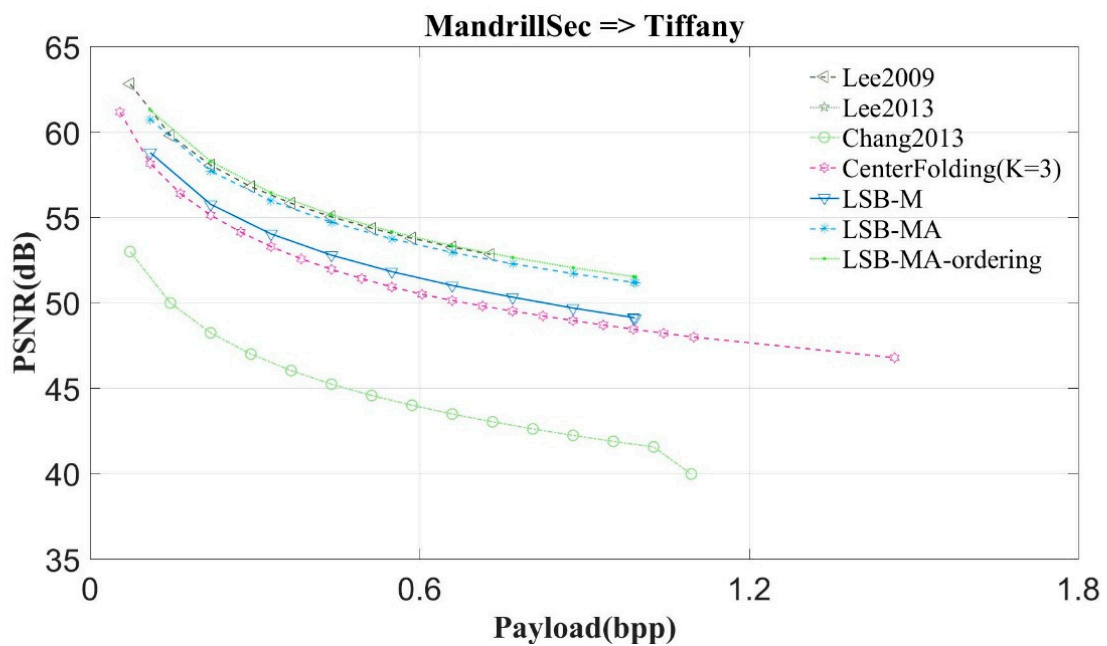


Figure 13. The experimental results of Tiffany with the secret image Mandrill.

From Figures 11 and 12 we can observe that the proposed scheme can get the highest image quality regardless of whether the image is complex or smooth. The experimental results of the other images have very similar curve to Lena. Hence, this study only shows the results of two images: Lena and Mandrill.

In the following experiment, this study used an image as the secret message to be concealed into the test image. Figure 13 shows the experimental results. The image quality of the proposed scheme is still the highest among the comparison schemes.

To test the efficient of the proposed scheme, this study statistics the probability of different pixels with different secret message by using three different types of secret messages. The first secret message was generated by the random number generator (RNG), the second and the third message were the fixed images ‘Tiffany’ and ‘CYUT Bird’, which

are shown in Figure 14. The statistic results are shown in Table 7. There are 16 different combinations composed by $LSB(A)$, $F(A, A)$, m_1 and m_2 . The column 'Count' is the total number of the occurrence of the combination, '%' is the percentage of the combination, LA' and LA'' are the operator to compute the stego-pixels A' and A'' , ' δ ' is the distortion made by LA' and LA'' , and 'TD' is the total number of distortion made by the combination. 'Total Distortion' in the end of the table is the total distance made by the secret image.



(a) Tiffany



(b) CYUT Bird

Figure 14. The fixed secret images 'Tiffany' and 'CYUT Bird'.

Form the table we can see that the count of each combination of the random number generate is almost the same. The average percentage is 6.25% and the standard deviation is 0.00049. The total number of the distortion made by the random number generate is 263,040. The count of the secret image 'Tiffany' is different from that of the RNG. The average percentage to embed $m_1 = 1$ and $m_2 = 1$ is 9.01%. The standard deviation is 0.02209. The total distortion of the secret image 'Tiffany' is 208,143, which is smaller than that of the RNG.

The count of each combination of the secret image 'CYUT Bird' is very different from the other two secret messages. Because the secret image has a lot of white pixels, which most significant bits start with '11' in the binary system. Hence, the probability of the pixel concealed with $m_1 = 1$ and $m_2 = 1$ is very high. The average percentage to embed $m_1 = 1$ and $m_2 = 1$ is 15.95%. The standard deviation is 0.05608. The total distortion of the secret image is 121,120, which is smallest of the three secret messages. Therefore, the image quality can be greatly improved especially for the secret image, which is not uniform.

Furthermore, although the proposed scheme needs to transmit the mapping table to the receiver for extracting the secret message and recovering the original image, the necessary extra information that needed to be transmitted is $\hat{\rho}$ and ρ of the mapping table. The scheme transforms the numbers of $\hat{\rho}$ into the binary system to form a binary string. There are 16 numbers of $\hat{\rho}$. The maximum value of $\hat{\rho}$ is 3. Hence, the scheme only uses two bits to encode the value. After encoded the total length of the binary string of $\hat{\rho}$ is $16 \times 2 = 32$ bits.

The values of ρ are also encoded to a binary string. The length of the string is also $16 \times 2 = 32$. Two binary strings are concatenated together to transmit to the receiver.

The receiver picks two bits up from the binary strings each time and transforms the bits into a decimal number to fill into the mapping table. If the value of $\hat{\rho}$ is equal to 0, then $LA' = 0$ and $LA'' = 0$. If the value of $\hat{\rho}$ is equal to 1, then $LA' = 0$ and $LA'' = 1$. If the value of $\hat{\rho}$ is equal to 2, then $LA' = 1$ and $LA'' = 0$. If the value of $\hat{\rho}$ is equal to 3 then $LA' = -1$ and $LA'' = 1$.

Therefore, the total number of the mapping table sent from the sender is $32 + 32 = 64$ (bits).

Table 7. The statistic results of the proposed used the random number and the fixed secret images ‘CYUT Bird’ and ‘Tiffany’.

LSB(A)	F(A, A)	m ₁	m ₂	Random Number Generator (RNG)						Secret Image: Tiffany						Secret Image: CYUT Bird					
				Count	%	LA'	LA''	δ	TD	Count	%	LA'	LA''	δ	TD	Count	%	LA'	LA''	δ	TD
0	0	0	0	16,180	6.17%	0	0	0	-	10,069	3.84%	-1	1	2	20,138	9191	3.51%	0	1	1	9191
		0	1	16,362	6.24%	0	1	1	16,362	11,265	4.30%	1	0	1	11,265	8040	3.07%	1	0	1	8040
		1	0	16,369	6.24%	1	0	1	16,369	20,508	7.82%	0	1	1	20,508	6544	2.50%	-1	1	2	13,088
		1	1	16,534	6.31%	-1	1	2	33,068	23,603	9.00%	0	0	0	-	41,670	15.90%	0	0	0	-
	1	0	0	16,235	6.19%	0	1	1	16,235	10,110	3.86%	-1	1	2	20,220	9137	3.49%	0	1	1	9137
		0	1	16,263	6.20%	0	0	0	-	11,445	4.37%	1	0	1	11,445	7934	3.03%	1	0	1	7934
		1	0	16,431	6.27%	-1	1	2	32,862	20,468	7.81%	0	1	1	20,468	6575	2.51%	-1	1	2	13,150
		1	1	16,463	6.28%	1	0	1	16,463	23,369	8.91%	0	0	0	-	41,746	15.92%	0	0	0	-
1	1	0	0	16,506	6.30%	1	0	1	16,506	10,237	3.91%	-1	1	2	20,474	9148	3.49%	0	1	1	9148
		0	1	16,585	6.33%	-1	1	2	33,170	11,283	4.30%	1	0	1	11,283	8298	3.17%	1	0	1	8298
		1	0	16,444	6.27%	0	1	1	16,444	20,434	7.79%	0	1	1	20,434	6560	2.50%	-1	1	2	13,120
		1	1	16,293	6.22%	0	0	0	-	23,874	9.11%	0	0	0	-	41,822	15.95%	0	0	0	-
	0	0	0	16,355	6.24%	-1	1	2	32,710	10,112	3.86%	-1	1	2	20,224	9150	3.49%	0	1	1	9150
		0	1	16,257	6.20%	1	0	1	16,257	11,218	4.28%	1	0	1	11,218	7836	2.99%	1	0	1	7836
		1	0	16,273	6.21%	0	0	0	-	20,466	7.81%	0	1	1	20,466	6514	2.48%	-1	1	2	13,028
		1	1	16,594	6.33%	0	1	1	16,594	23,683	9.03%	0	0	0	-	41,979	16.01%	0	0	0	-
Total distortion:				263,040						208,143						121,120					

In 2001, Fridrich et al. [27] proposed the use of RS steganalysis to detect whether an image has a secret message in it [28]. The technology uses a judgment function and a flipping function to divide the pixels into two groups. The judgment function separates the groups into two types, based on smoothness and regularity. The flipping function segregates the groups into three categories: Regular (R), Singular (S), and Unusable (U). The technology applies two masks $M = [1\ 0\ 0\ 1]$ and $-M = [-1\ 0\ 0\ -1]$ to calculate the percentages of regular, singular, and unusable that are marked by R_FM_G, R_M_G, S_FM_G, S_M_G, U_FM_G, and U_M_G, respectively. The hypotheses are $R_M_G \cong R_FM_G$, $S_M_G \cong S_FM_G$, and $U_M_G \cong U_FM_G$. Figures 15 and 16 are the RS steganalysis results of Mandrill.

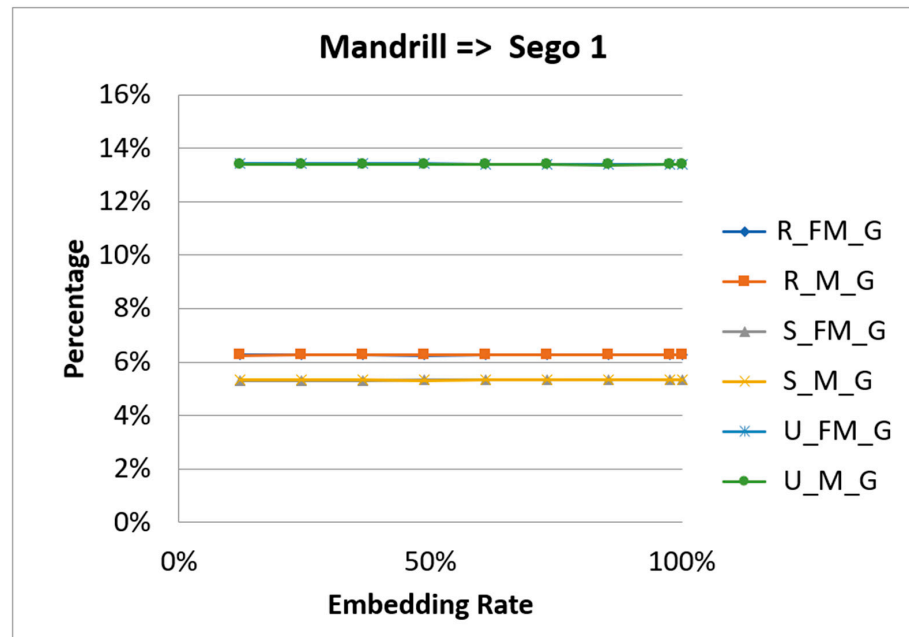


Figure 15. The RS analysis result of the first stego image of Mandrill.

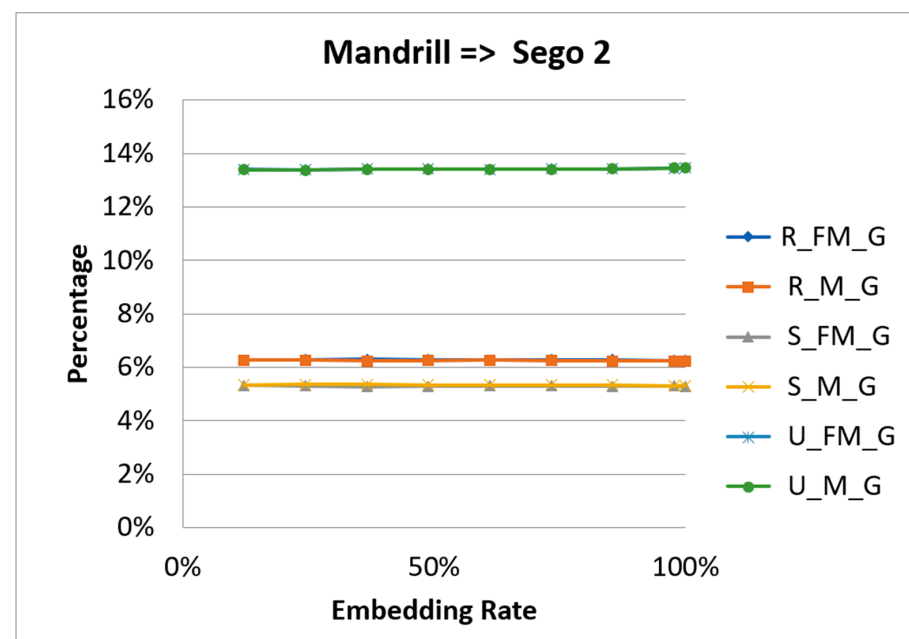


Figure 16. The RS analysis result of the second stego image of Mandrill.

From the figures, we can see that the curve of R_M_G is close to that of R_FM_G. The curves of S_M_G, S_FM_G, U_M_G, and U_FM_G have the same shapes. Therefore, the proposed scheme can against the RS steganalysis.

5. Conclusions and Future Works

In this paper, a modified LSB matching method using the dual-image and likelihood recording strategy is proposed. The scheme analyzes all possible modifications under all hidden conditions and re-encodes each combination according to the frequency of its occurrence. The combination with a higher occurrence rate is re-encoded with a lower modification rule. The experimental results show that the embedding capacity of the proposed method is like the method used in Tseng et al.'s scheme. Moreover, the image quality of the proposed scheme is the highest among the comparison methods. Furthermore, the proposed scheme against the steganalysis attacks.

The reason why the proposed scheme can get higher image quality is because the scheme transforms the worst cases with better encode results. In general, each worst case may make two images distance where one pixel is -1 and the other one is +1. That means the case will generate $2^2 = 4$ squared errors for computing the image quality. In the proposed scheme, the worst case is re-encoded with the minimum distortion code 0. Hence, the stego-pixel is the same with the original one such that the image distance is 0. The image distortion can be effectively reduced. The proposed scheme is especially suitable for simple secret image such as logo, cartoons, and signature. On the contrary, the proposed scheme can only get a few increasing while the secret image is a uniform image.

In the future, we will try to figure out how to re-encode the secret image according to its characteristic. The scheme needs adaptively or elastically change the encoding strategy such as running encoding or Huffman coding, to encode the different cases to further reduce the image distortion, or filter the bad cases, which will cause huge damage in the pre-processing procedure. Furthermore, add more translation tables to improve the image quality.

Author Contributions: T.-C.L. created the idea, wrote the paper, corrected the program; P.-C.Y. wrote the paper, run the program; B.J. write the paper, corrected the paper. All authors have read and agreed to the published version of the manuscript.

Funding: Ministry of Science and Technology (MOST), Taiwan, Republic of China MOST 109-2221-E-324-025-MY3.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors gratefully acknowledge the financial support of this study from the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under the Grant MOST 109-2221-E-324 -025 -MY3. The authors also want to thank the reviewers who give us great review comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hussain, M.; Wahab, A.W.A.; Idris, Y.I.B.; Ho, A.T.; Jung, K.H. Image Steganography in Spatial Domain: A Survey. *Signal Process. Image Commun.* **2018**, *65*, 46–66. [[CrossRef](#)]
2. Liao, X.; Shu, C. Reversible Data Hiding in Encrypted Images Based on Absolute Mean Difference of Multiple Neighboring Pixels. *J. Vis. Commun. Image Represent.* **2015**, *28*, 21–27. [[CrossRef](#)]
3. Qin, C.; Chang, C.C.; Hsu, T.J. Reversible Data Hiding Scheme Based on Exploiting Modification Direction with Two Steganographic Images. *Multimed. Tools Appl.* **2015**, *74*, 5861–5872. [[CrossRef](#)]
4. Chen, X.Y.; Gao, G.Y.; Liu, D.D.; Xia, Z.H. Steganalysis of LSB Matching Using Characteristic Function Moment of Pixel Differences. *China Commun.* **2016**, *13*, 66–73. [[CrossRef](#)]
5. Jana, B. Dual Image Based Reversible Data Hiding Scheme Using Weighted Matrix. *Int. J. Electron. Inf. Eng.* **2016**, *5*, 6–19.

6. Lee, C.F.; Wang, K.H.; Chang, C.C.; Huang, Y.L. A Reversible Data Hiding Scheme Based on Dual Steganographic Images. In Proceedings of the Third International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 15–16 January 2009; pp. 228–237.
7. Lee, C.F.; Huang, Y.L. Reversible Data Hiding Scheme Based on Dual Stegano-Images Using Orientation Combinations. *Telecommun. Syst.* **2013**, *52*, 2237–2247. [[CrossRef](#)]
8. Lu, T.C.; Chang, T.C.; Shen, J.J. An Effective Maximum Distortion Controlling Technology in the Dual-Image-Based Reversible Data Hiding Scheme. *IEEE Access* **2020**, *8*, 90824–90837. [[CrossRef](#)]
9. Lu, T.C.; Wu, J.H.; Huang, C.C. Dual-Image-Based Reversible Data Hiding Method Using Center Folding Strategy. *Signal Process.* **2015**, *115*, 195–213. [[CrossRef](#)]
10. Sahu, A.K.; Swain, G. A Review on LSB Substitution and PVD Based Image Steganography Techniques. *Indones. J. Electr. Eng. Comput. Sci.* **2016**, *2*, 712–719. [[CrossRef](#)]
11. Sahu, A.K.; Swain, G. An Improved Data Hiding Technique Using Bit Differencing and LSB Matching. *Internetworking Indones. J.* **2018**, *10*, 17–21.
12. Sahu, A.K.; Swain, G.; Babu, E.S. Digital Image Steganography Using Bit Flipping. *Cybern. Inf. Technol.* **2018**, *18*, 69–80. [[CrossRef](#)]
13. Shaji, C.; Shatheesh, I. Dual Encoding Approach with Sequence Folding for Reversible Data Hiding in Dual Stego Images. *Multimed. Tools Appl.* **2021**, *80*, 13595–13614. [[CrossRef](#)]
14. Jafar, F.; Darabkh, K.A.; Al-Zubi, R.T.; Saifan, R.R. An Efficient Reversible Data Hiding Algorithm Using Two Steganographic Images. *Signal Process.* **2016**, *128*, 98–109. [[CrossRef](#)]
15. Jung, K.H. Dual Image Based Reversible Data Hiding Method Using Neighbouring Pixel Value Differencing. *Imaging Sci. J.* **2015**, *63*, 398–407. [[CrossRef](#)]
16. Kumar, A.S.; Swain, G. Dual Stego-imaging Based Reversible Data Hiding Using Improved LSB Matching. *Int. J. Intell. Eng. Syst.* **2019**, *12*, 63–74.
17. Kumar, A.S.; Swain, G. Reversible Image Steganography Using Dual-Layer LSB Matching. *Sens. Imaging* **2020**, *21*, 1.
18. Fadil, A.J. An Extensive Analysis and Conduct Comparative Based on Statistical Attach of LSB Substitution and LSB Matching. *Int. J. Eng. Technol.* **2020**, *7*, 4008–4023. [[CrossRef](#)]
19. Hiary, H.; Sabri, K.E.; Mohammed, M.S. A Hybrid Steganography System Based on LSB Matching and Replacement. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 374–380. [[CrossRef](#)]
20. Kumar, A.; Swain, G. High Fidelity Based Reversible Data Hiding Using Modified LSB Matching and Pixel Difference. *J. King Saud Univ. Comput. Inf. Sci.* **2019**. [[CrossRef](#)]
21. Hwang, M.S.; Xie, M.R.; Wu, C.C. A Reversible Hiding Technique Using LSB Matching for Relational Databases. *Informatica* **2020**, *31*, 481–497. [[CrossRef](#)]
22. Mielikainen, J. LSB Matching Revisited. *IEEE Signal Process. Lett.* **2006**, *13*, 285–287. [[CrossRef](#)]
23. Yang, G.; Li, X.; Li, B.; Guo, Z. A New Detector of LSB Matching Steganography Based on Likelihood Ratio Test for Multivariate Gaussian Covers. In Proceedings of the 2015 Asia Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Hong Kong, China, 6–19 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 757–760.
24. Lu, T.C.; Tseng, C.Y.; Wu, J.H. Dual Imaging-based Reversible Hiding Technique Using LSB Matching. *Signal Process.* **2015**, *108*, 77–89. [[CrossRef](#)]
25. Tseng, H.W.; Lu, H.X.; Leng, H.S. Dual Image Reversible Data Hiding Based on Modified LSB Matching Method. *Recent Adv. Intell. Inf. Hiding Multimed. Signal Process.* **2019**, *109*, 256–263.
26. Wang, Y.L.; Shen, J.J.; Hwang, M.S. An Improved Dual Image-Based Reversible Hiding Technique Using LSB Matching. *Int. J. Netw. Secur.* **2017**, *19*, 858–862.
27. Fridrich, J.; Goljan, M. Practical Steganalysis of Digital Images—State of the Art. In Proceedings of the SPIE—The International Society for Optical Engineering, San Jose, CA, USA, 27 December 2002; Volume 4675.
28. Swain, G. Digital Image Steganography Using Eight Directional PVD against RS Analysis and PDH Analysis. *Adv. Multimed.* **2018**, *2018*, 1–13. [[CrossRef](#)]