symmetry

MDPI

Article

Efficient Information Hiding Based on Theory of Numbers

Yanjun Liu [1], Chin-Chen Chang [1,*], Peng-Cheng Huang [1,2] and Cheng-Yi Hsu [1]

[1] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan; yjliu104@gmail.com (Y.L.); pc4hpc@gmail.com (P.-C.H.); eirc610421@gmail.com (C.-Y.H.)
[2] Department of Computer Science, Xiamen University of Technology, Xiamen 361024, China
* Correspondence: alan3c@gmail.com; Tel.: +886-4-2451-7250 (ext. 3790)

Received: 2 December 2017; Accepted: 3 January 2018; Published: 8 January 2018

Abstract: Data hiding is an efficient technique that conceals secret data into a digital medium. In 2006, Zhang and Wang proposed a data hiding scheme called exploiting modification direction (EMD) which has become a milestone in the field of data hiding. In recent years, many EMD-type data hiding schemes have been developed, but their embedding capacity remains restricted. In this paper, a novel data hiding scheme based on the combination of Chinese remainder theorem (CRT) and a new extraction function is proposed. By the proposed scheme, the cover image is divided into non-overlapping pixel groups for embedding to increase the embedding capacity. Experimental results show that the embedding capacity of the proposed scheme is significantly higher (greater than 2.5 bpp) than previously proposed schemes while ensuring very good visual quality of the stego image. In addition, security analysis is given to show that the proposed scheme can resist visual attack.

Keywords: data hiding; exploiting modification direction (EMD); Chinese remainder theorem (CRT); extraction function; embedding capacity

1. Introduction

The rapid developments of computer and network technologies led to an explosion in the transmission of digital information over the Internet. The digital information mostly contains sensitive and confidential contents that can be intercepted or tampered with during transmission. Therefore, ensuring secure information communication has become a very important issue. There are two main approaches to achieve this goal. One approach is cryptography [1], in which the message is encrypted with a secret key and only the holder of the secret key can decrypt the cipher text to recover the original message. RSA public-key cryptosystem using a pair of keys is the most widely used cryptography. A public key is paired with a private key that is known only to the expected message receiver. The sender encrypts a message with the public key and only the receiver who has the paired private key can decrypt it. Unfortunately, disclosure of the message may happen if the private key leaks. The other approach for information security is data hiding, and this has attracted a lot of attention over the past few years [2–5].

Data hiding [2,3] is an efficient technique that conceals secret data into a medium. The differences in the image before and after concealing data are so tiny that it is impossible for an observer to visually perceive the presence of hidden data. A good data hiding scheme should both maintain good image quality and preserve sufficient embedding capacity. However, it is difficult to satisfy the two requirements at the same time in most cases. It is generally true that the image distortion increases when the embedding capacity increases; on the other hand, the image quality is enhanced at the cost of the embedding capacity. Therefore, how to achieve a satisfactory balance between the image quality

and the embedding capacity has become a technically challenging topic and many researchers have proposed various data hiding methods [4–6] focusing on this topic.

Data hiding for digital images is basically developed in three domains—the spatial domain, the frequency domain and the compression domain. In the frequency domain, the cover image is transformed into frequency coefficients via various discrete transform functions such as discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT). The primary property of frequency domain data is that low frequency coefficients contain more important information, whereas in high frequency areas, information is less significant. Thus, the matrix of frequency coefficients are divided into non-overlapping blocks and the secret data will be embedded in those blocks. For data hiding in compression domain, the frequently used compression technologies include vector quantization (VQ), block truncation coding (BTC) and joint photographic experts group (JPEG). A milestone in the history of spatial domain-based data hiding is the method of least-significant-bit (LSB) replacement [2]. LSB method is very simple as it just replaces the LSBs in a cover image with secret bits to produce a stego image. The embedding capacity is satisfactory along with a good image quality, but it is very vulnerable to statistical analysis of the stego image. Westfeld and Pfitzmann [3] found that the statistics for the frequencies of neighboring pixel value pairs in the stego image can easily detect the presence of hidden data. To resist statistical attack, LSB matching [4] was introduced. It improves the way of modifying the cover image such that the value of the cover pixel is either randomly increased or decreased by one in case the LSB of the cover pixel is not identical to the secret bit. Later, Mielikainen [5] exploited the direction of modification to the cover pixels for the first time to enhance the LSB matching scheme. A cover pixel pair is used as a minimal unit to embed two consecutive secret bits according to a binary function. This scheme outweighs LSB matching in terms of security and image quality degradation while keeping the same embedding capacity. However, Zhang and Wang [6] pointed out that Mielikainen's scheme [5] does not fully exploit the modification directions, and they presented a novel data hiding scheme called the exploiting modification direction (EMD) scheme. The EMD scheme first converts binary secret data into a $(2m + 1)$-ary stream of secret digits, and then uses a group of m adjacent pixels to carry one secret digit. Only one pixel value in the group is $+1$ or -1 according to a new extraction function, thereby achieving very good image quality. The weakness of the EMD scheme is that the embedding capacity decreases drastically if the number of pixels in a group increases.

In recent years, many data hiding schemes that are inspired by the concept of EMD have been proposed to increase the embedding capacity [7–21]. Lee et al.'s scheme [7] employed a pixel segmentation strategy to provide a larger payload than that of EMD, but this suffers from worse image quality. Chang et al. [8] introduced a novel scheme based on EMD and Sudoku solutions. Each cover pixel pair conceals one secret digit in the nonary numeral system by the reference matrix according to a selected Sudoku solution. The scheme can achieve a higher embedding capacity of 1.5 bits per pixel (bpp) and a very good image quality. Moreover, the scheme is more secure than the EMD method since it is very difficult to determine which Sudoku solution is selected from a large number of possible solutions. To minimize the image distortions, Hong et al. [9] proposed a new scheme that searches embeddable positions using the nearest Euclidean distance, leading to a better image quality than that of Chang et al.'s scheme [8] under the same embedding capacity. In 2010, Kim et al. [10] introduced an EMD-2 scheme that changes the values of at most two pixels in a group. Experimental results showed that EMD-2 is superior to EMD in larger payloads with similar image distortions. In 2014, Chang et al. [11] proposed a novel data hiding scheme originating from EMD and turtle shell structure. The binary secret stream can be embedded directly in such a way that three secret bits are embedded in a pair of consecutive cover pixels with the guidance of a reference matrix based on turtle shells. Experimental results revealed that this scheme has a higher embedding capacity than EMD and Kim et al.'s scheme [10]. Also, it outperforms EMD, Chang et al.'s scheme [8] and Hong et al.'s scheme [9] in better image quality under the same embedding capacity. Later, Liu et al. [12] improved Chang et al.'s scheme [11] by constructing a location table from the turtle shell-based reference matrix

to guide the modification of cover pixel pairs. This scheme achieves very good image quality above 45 dB and is better than Chang et al.'s scheme [11] with higher embedding capacity.

Recently, Kuo et al. proposed a series of EMD-type schemes [15–17] to further improve the EMD method. In order to increase the embedding capacity, a generalized EMD (GEMD) scheme was introduced in [16]. Unlike the EMD, the GEMD does not require the conversion of the binary secret data before embedding so as to accelerate the embedding speed. The GEMD scheme maintains better embedding capacity than EMD under different pixel group sizes. Later, a modified signed digit (MSD) scheme [17] for data hiding was proposed that restricts the number of modified pixels to $\lceil m/2 \rceil$ when the group size is m, while all group pixels may be changed in GEMD. Unfortunately, MSD sacrifices the embedding capacity to obtain better image quality than GEMD. Recently, Kuo et al. [18] proposed a new EMD-type scheme called binary power EMD (BPEMD) in which both the coefficient and modulus of the extraction function are binary power. Experimental results reveal that BPEMD has higher embedding capacity than EMD and MSD and withstands well-known attacks.

In order to further increase the embedding capacity, we propose an EMD-type data hiding scheme based on Chinese remainder theorem (CRT) [22]. CRT can make a solution to determine an integer by the given system of simultaneous congruencies in number theory. Nowadays, CRT is used extensively in secret sharing and other applications of information security [22–24]. Fortunately, we also find that CRT is very suitable for data hiding. To the best of our knowledge, no EMD-type schemes employing CRT has been proposed. In this paper, for the first time, we propose a high capacity data hiding scheme from the combination of CRT and a new extraction function. The characteristics of the proposed scheme are listed below:

1. It is the first EMD-type data hiding scheme that uses CRT as its main building block. The cover image is divided into non-overlapping m-pixel groups for embedding data. According to the CRT and a new extraction function, the ith cover pixel in a group can directly embed $(i+1)$ binary secret bits;
2. The coefficients of the constructed extraction function are pairwise coprime integers and the modulus is the product of the coefficients, which is different from the extraction functions of previous EMD-type schemes. Therefore, for data extraction, the embedded secret data is first computed by the extraction function and then retrieved by a modular operation according to the CRT. This two layer embedding strategy can further increase the security;
3. The embedding capacity of the proposed scheme is significantly high while guaranteeing good image quality. In particular, the embedding capacity can maintain at least 2.5 bpp and increase when the number of cover pixels in a group increases.

The rest of the paper is organized as follows. Section 2 briefly reviews typical EMD-type data hiding schemes and basic knowledge about CRT. Section 3 describes our proposed data hiding scheme. Experimental results are provided in Section 4, and conclusions are given in Section 5.

2. Preliminaries

In this section, we first give a review of typical EMD-type data hiding schemes, such as EMD [6], GEMD [16] and BPEMD [18]. Then, we introduce essential knowledge about CRT since it is the most important building element of our proposed scheme.

2.1. EMD Data Hiding Scheme

The EMD scheme proposed by Zhang and Wang [6] embeds one secret digit in a $(2m + 1)$-ary numeral system into m cover pixels, among which at most one pixel is +1 or -1. Let a vector $P_m = [p_1, p_2, \ldots, p_m]$ denote a group of m pixel values and P_m in an m-dimensional space corresponds

to a value of an extraction function g_E, which is computed by the following equation as a weighed sum modulo $(2m+1)$:

$$g_E(p_1, p_2, \ldots, p_m) = \left(\sum_{i=1}^{m} p_i \cdot i\right) \bmod (2m+1). \quad (1)$$

According to the extraction function g_E, the EMD embedding algorithm (Algorithm 1) is shown as follows:

Algorithm 1 EMD Embedding Algorithm [6].

Input: cover image I_c and binary secret data stream S
Output: stego image I_s

Step 1. Convert binary secret data stream S to a $(2m+1)$-ary stream S'. First, S is divided into a sequence of segments with l bits. Then, each l-bit segment is converted to r digits in a $(2m+1)$-ary numeral system, where

$$l = \lfloor r \cdot \log_2(2m+1) \rfloor. \quad (2)$$

Step 2. Divide the cover image I_c into non-overlapping groups, each of which consists of m adjacent pixels.

Step 3. Obtain an m-pixel group $(p_1, p_2, \ldots, p_m)$ from I_c and one digit t from S'.

Step 4. Compute $y = g_E(p_1, p_2, \ldots, p_m)$ by Equation (1) and obtain the difference $D_E = (t-y) \bmod (2m+1)$.

Step 5. If $D_E = 0$, set $p'_i = p_i$ for $i \in \{1, 2, \ldots, m\}$, where p'_i is the stego pixel. If $D_E \neq 0$ and $D_E \leq m$, set $p'_{D_E} = p_{D_E} + 1$ and $p'_i = p_i$ for $i \in \{1, 2, \ldots, m\}$ and $i \neq D_E$. If $D_E \neq 0$ and $D_E > m$, set $p'_{2m+1-D_E} = p_{2m+1-D_E} - 1$ and $p'_i = p_i$ for $i \in \{1, 2, \ldots, m\}$ and $i \neq (2m+1-D_E)$.

Step 6. Repeat Steps 3–5 until all secret data is embedded.

For the extraction, we retrieve all m-pixel group $(p'_1, p'_2, \ldots, p'_m)$ from the stego image I_s, and then compute $s = g_E(p'_1, p'_2, \ldots, p'_m)$ for each group. Obviously, s is one digit in the $(2m+1)$-ary secret stream S'. Finally, S' is converted back to the binary secret stream S. Here, we give an example to illustrate how to embed secret data using the EMD scheme.

Example 1. *Given three grayscale pixels* $(28, 35, 38)$ *of a cover image and a binary secret data stream* $S = (0101)_2$, *embed S into the above three-pixel group using EMD when* $m = 3$.

First, compute one digit $t = (0101)_2 = (5)_7$. Then, compute $y = g_E(p_1, p_2, p_3) = (28 \times 1 + 35 \times 2 + 38 \times 3) \bmod 7 = 2$. Thus, the difference $D_E = (t-y) \bmod (2m+1) = (5-2) \bmod 7 = 3$ is obtained. Because $D_E = m$, we set $p'_1 = p_1 = 28$, $p'_2 = p_2 = 35$ and $p'_3 = p_3 + 1 = 39$ in the stego image. To extract the hidden data, we just compute $s = g_E(p'_1, p'_2, p'_3) = (28 \times 1 + 35 \times 2 + 39 \times 3) \bmod 7 = 5 = (0101)_2$.

2.2. GEMD Data Hiding Scheme

From the EMD scheme, we can infer that its largest embedding capacity is achieved at 1.16 bpp when there are two pixels in a group. The embedding capacity decreases drastically if the size of the pixel group increases. To enhance the embedding capacity, Kuo and Wang [16] proposed the GEMD scheme. GEMD has two main contributions: (1) it does not require the conversion of the binary secret data to a specified numeral stream before embedding; and (2) its embedding capacity stays greater than 1 bpp when the size of pixel group increases. A new extraction function g_G is introduced in GEMD as follows:

$$g_G(p_1, p_2, \ldots, p_m) = \left(\sum_{i=1}^{m} p_i \cdot (2^i - 1)\right) \bmod 2^{m+1}. \quad (3)$$

According to the extraction function g_G, the GEMD embedding algorithm (Algorithm 2) is shown below:

Algorithm 2 GEMD Embedding Algorithm [16].

Input: cover image I_c and binary secret data stream S
Output: stego image I_s

Step 1. Divide the cover image I_c into non-overlapping groups, each of which consists of m adjacent pixels.
Step 2. Obtain an m-pixel group $(p_1, p_2, \ldots, p_m)$ from I_c.
Step 3. Read $(m+1)$ secret bits from S and obtain the corresponding (2^{m+1})-ary secret data t.
Step 4. Compute $y = g_G(p_1, p_2, \ldots, p_m)$ by Equation (3) and obtain the difference $D_G = (t-y) \bmod 2^{m+1}$.
Step 5. If $D_G = 2^m$, set $p'_1 = p_1 + 1$, $p'_m = p_m + 1$ and $p'_i = p_i$ for $i \in \{2, 3, \ldots, m-1\}$, where p'_i is the stego pixel, and then go to Step 8; else if $D_G < 2^m$, go to Step 6; else go to Step 7.
Step 6. Transform D_G to $(m+1)$-bit data $(d_{m+1} d_m \ldots d_2 d_1)_2$.

For $i = 1$ to m do

If ($d_{i+1} = 0$ and $d_i = 1$) then $p'_i = p_i + 1$;

else if ($d_{i+1} = 1$ and $d_i = 0$) then $p'_i = p_i - 1$;

else $p'_i = p_i$.

End For.

Go to Step 8.

Step 7. Compute $D_G = 2^{m+1} - D_G$ and then transform D_G to $(m+1)$-bit data $(d_{m+1} d_m \ldots d_2 d_1)_2$.

For $i = 1$ to m do

If ($d_{i+1} = 0$ and $d_i = 1$) then $p'_i = p_i - 1$;

else if ($d_{i+1} = 1$ and $d_i = 0$) then $p'_i = p_i + 1$;

else $p'_i = p_i$.

End For.

Step 8. Go to Step 2 until all secret data is embedded.

Similar to the EMD scheme, the GEMD scheme extracts the secret data by computing the extraction function g_G using stego pixels as its inputs. To make a clear comparison between GEMD and EMD, we still take Example 1 to demonstrate the embedding and extracting processes using GEMD when $m = 3$.

In the embedding process of GEMD, first, obtain 16-ary secret data $t = (0101)_2 = (5)_{16}$. Then, compute $y = g_G(p_1, p_2, p_3) = (28 \times 1 + 35 \times 3 + 38 \times 7) \bmod 16 = 15$. Thus, the difference $D_G = (t-y) \bmod 2^{m+1} = (5-15) \bmod 16 = 6$ is obtained. Because $D_G < 2^m = 8$, transform D_G to $(0110)_2$. According to Step 6, we set $p'_1 = p_1 - 1 = 27$, $p'_2 = p_2 = 35$ and $p'_3 = p_3 + 1 = 39$ in the stego image. To extract the hidden data, we just compute $s = g_G(p'_1, p'_2, p'_3) = (27 \times 1 + 35 \times 3 + 39 \times 7) \bmod 16 = 5 = (0101)_2$.

2.3. BPEMD Data Hiding Scheme

Unlike the aforementioned EMD-type schemes, both the coefficient and modulus of the extraction function are binary power in the BPEMD scheme (Algorithm 3) [18]. Since the multiplication of binary numbers implemented by shifting bits is faster than that of numbers in other radices, BPEMD can speed up the embedding process. Experimental results show that embedding capacity of BPEMD is quite similar to that of GEMD but higher than that of EMD and MSD. The extraction function g_B in BPEMD is shown below:

$$g_B(p_1, p_2, \ldots, p_m) = \left(\sum_{i=1}^{m} p_i \cdot 2^{i-1} \right) \bmod 2^{m+1}. \quad (4)$$

Algorithm 3 BPGEMD Embedding Algorithm [18].

Input: cover image I_c and binary secret data stream S
Output: stego image I_s

Step 1. Divide the cover image I_c into non-overlapping groups, each of which consists of m adjacent pixels.
Step 2. Obtain an m-pixel group $(p_1, p_2, \ldots, p_m)$ from I_c.
Step 3. Read $(m+1)$ secret bits from S and obtain the corresponding (2^{m+1})-ary secret data t.
Step 4. Compute $y = g_B(p_1, p_2, \ldots, p_m)$ by Equation (4) and obtain the difference $D_B = (t - y) \bmod 2^{m+1}$.
Step 5. If $D_B = 2^m$, set $p'_m = p_m + 2$ and $p'_i = p_i$ for $i \in \{1, 2, \ldots, m-1\}$, where p'_i is the stego pixel, and then go to Step 8; else if $D_B < 2^m$, go to Step 6; else go to Step 7.
Step 6. Transform D_B to m-bit data $(d_m d_{m-1} \ldots d_2 d_1)_2$.

For $i = 1$ to m do $p'_i = p_i + d_i$.

Go to Step 8.
Step 7. Compute $D_B = 2^{m+1} - D_B$ and then transform D_B to m-bit data $(d_m d_{m-1} \ldots d_2 d_1)_2$.

For $i = 1$ to m do $p'_i = p_i - d_i$.
Step 8. Go to Step 2 until all secret data is embedded.

From the embedding algorithm of BPEMD, it can be implied that p_m can be modified by $\{-1, 0, 1, 2\}$, whereas p_i for $i \neq m$ can be modified by $\{-1, 0, 1\}$. Obviously, the secret data can be extracted easily by calculating the extraction function g_B with stego pixels as its inputs. Here, we also use Example 1 to explain the BPGEMD scheme with $m = 3$.

For the embedding, after obtaining 16-ary secret data $t = (0101)_2 = (5)_{16}$, we compute $y = g_B(p_1, p_2, p_3) = (28 \times 1 + 35 \times 2 + 38 \times 4) \bmod 16 = 10$. Thus, the difference $D_B = (t - y) \bmod 2^{m+1} = (5 - 10) \bmod 16 = 11$ is obtained. Because $D_B > 2^m = 8$, we compute $D_B = 2^{m+1} - D_B = 16 - 11 = 5$ and then transform it to $(101)_2$. According to Step 7, we set $p'_1 = p_1 - 1 = 27$, $p'_2 = p_2 = 35$ and $p'_3 = p_3 - 1 = 37$ in the stego image. To extract the hidden data, we just compute $s = g_B(p'_1, p'_2, p'_3) = (27 \times 1 + 35 \times 2 + 37 \times 4) \bmod 16 = 5 = (0101)_2$.

2.4. Chinese Remainder Theorem

The CRT [22–24], resulting from Bézout's Lemma [25], is an approach to determine an integer in a specific range by the given system of simultaneous congruencies in number theory. CRT is used as a main building block in our proposed scheme and described as follows. Given n positive, pairwise coprime integers, $q_1, q_2, \ldots, q_n$, and n positive integers, $x_1, x_2, \ldots, x_n$, for $x_i < q_i$, a system of equations can be established for determining an integer X:

$$\begin{aligned} x_1 &= X \bmod q_1, \\ x_2 &= X \bmod q_2, \\ &\vdots \\ x_n &= X \bmod q_n. \end{aligned}$$

Therefore, the unique solution X in Z_P is computed by CRT as $X = \sum_{i=1}^{n} M_i \cdot M'_i \cdot x_i \bmod \prod_{i=1}^{n} q_i$, where $M_i = \frac{\prod_{i=1}^{n} q_i}{q_i}$ and $M_i \cdot M'_i \equiv 1 (\bmod q_i)$.

3. Proposed CRT-Based Scheme for Data Hiding

In this section, we propose a novel EMD-type data hiding scheme based on CRT called CRT-EMD. In the proposed scheme, the cover image is divided into non-overlapping m-pixel groups. According to the CRT and a new extraction function, the ith cover pixel in a group can directly embed $(i+1)$ secret bits so as to achieve high embedding capacity. In particular, the feasibility of data embedding by our

proposed scheme is addressed in Section 3.1. In Sections 3.2 and 3.3, we elaborate the embedding and extracting processes of the proposed scheme, respectively.

3.1. Feasibility Study

In our proposed data hiding scheme, an extraction function which is quite different from those of previous EMD-type schemes is constructed as follows:

$$g_C(p_1, p_2, \ldots, p_m) = \left(\sum_{i=1}^{m} p_i \cdot q_i \right) \bmod \prod_{i=1}^{m} q_i, \tag{5}$$

where $(p_1, p_2, \ldots, p_m)$ is an m-pixel group in the cover image and $q_1, q_2, \ldots, q_m$ are m positive, pairwise coprime integers with $q_i \geq 2^{i+1}$ for $1 \leq i \leq m$. Denote the (2^{i+1})-ary value of $(i+1)$ secret bits carried by p_i as b_i, where $1 \leq i \leq m$. Now the key issue is whether it is feasible to modify p_i for embedding b_i while minimizing the image distortion. In this subsection, we will analyze the feasibility of the above issue by using CRT.

Let $y = g_C(p_1, p_2, \ldots, p_m)$ and thus the value of y is obviously in the range of $[0, \prod_{i=1}^{m} q_i)$. Assume there is an integer y' also in the range of $[0, \prod_{i=1}^{m} q_i)$. Then, we can establish the following equations:

$$\begin{aligned} b_1 &= y' \bmod q_1, \\ b_2 &= y' \bmod q_2, \\ &\vdots \\ b_m &= y' \bmod q_m, \end{aligned} \tag{6}$$

and easily compute the value of y' by CRT. Therefore, if we can change y to y' through modifying $p_1, p_2, \ldots, p_m$, the secret data b_i can successfully be embedded in p_i. Let $D_C = (y' - y) \bmod \prod_{i=1}^{m} q_i$ and the modification on p_i be ε_i ($\varepsilon_i \in N$). Therefore, we must prove

$$q_1 \cdot \varepsilon_1 + q_2 \cdot \varepsilon_2 + \cdots + q_m \cdot \varepsilon_m = D_C \tag{7}$$

to ensure that y can be modified to y'.

In the following, we apply Bézout's Lemma (also called Bézout's identity) [25], a famous theorem in number theory, to prove Equation (7). Bézout's Lemma is described as follows:

Bézout's Lemma [25]. *Let a_1 and a_2 be nonzero integers and denote h as their greatest common divisor. Then there exist two integers y_1 and y_2 such that*

$$a_1 \cdot y_1 + a_2 \cdot y_2 = H, \tag{8}$$

where H is a multiple of h.

It should be noticed that the integer pair (y_1, y_2) is not unique. When one pair of solution (y_1, y_2) has been computed, all pairs can be obtained by

$$y_1 = y_1 + k \cdot \frac{a_2}{h}, \tag{9}$$

$$\text{and } y_2 = y_2 - k \cdot \frac{a_1}{h}, \tag{10}$$

where k is an arbitrary integer. Let a pair of solutions (y_1, y_2) that minimize the value of $(|y_1| + |y_2|)$ be called **minimal solution**. Bézout's Lemma has an attractive property that it is very easy to determine the minimal solution. In fact, exactly two pairs of all the solutions satisfy $|y_1| \leq |a_2/h|$ and

$|y_2| \leq |a_1/h|$. The extended Euclidean algorithm [25] always produces one of the above two pairs from which the minimal solution can be obtained immediately.

Lemma 1 [25]. *Let c_1 and c_2 be coprime integers and H' be a nonzero integer. Then there exist two integers y_1 and y_2 such that*

$$c_1 \cdot y_1 + c_2 \cdot y_2 = H'. \tag{11}$$

Proof. Since the integers c_1 and c_2 are coprime, their greatest common divisor h is "1". According to Bézout's Lemma, we can infer that $c_1 \cdot y_1 + c_2 \cdot y_2 = H' \cdot h = H'$. Therefore, Lemma 1 is a special case of Bézout's Lemma when a_1 and a_2 are coprime integers. □

Both Bézout's Lemma and Lemma 1 can be extended to more than two integers as follows:

Lemma 2 [25]. *Let $a_1, a_2, \ldots, a_n$ be n nonzero integers and denote h as their greatest common divisor. Then there exist integers $y_1, y_2, \ldots, y_n$ such that*

$$a_1 \cdot y_1 + a_2 \cdot y_2 + \cdots + a_n \cdot y_n = H, \tag{12}$$

where H is a multiple of h.

Lemma 3 [25]. *Let $c_1, c_2, \ldots, c_n$ be pairwise coprime integers and H' be a nonzero integer. Then there exist integers $y_1, y_2, \ldots, y_n$ such that*

$$c_1 \cdot y_1 + c_2 \cdot y_2 + \cdots + c_n \cdot y_n = H'. \tag{13}$$

Now we present a very important theorem regarding our proposed scheme.

Theorem 1. *In the CRT-EMD data hiding scheme, there exist integers, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$, satisfying $q_1 \cdot \varepsilon_1 + q_2 \cdot \varepsilon_2 + \ldots + q_m \cdot \varepsilon_m = D_C$ (Equation (7)). In addition, a minimal solution that minimizes the value of $(|\varepsilon_1| + |\varepsilon_2| + \ldots + |\varepsilon_m|)$ can be obtained.*

Proof. According to the CRT-EMD scheme, there are two integers y and y' in the same range of $[0, \prod_{i=1}^{m} q_i)$, where $y = g_C(p_1, p_2, \ldots, p_m)$ and y' is computed by CRT through Equation (6). Let $D_C = y' - y$ and the modification on the cover pixel p_i be ε_i ($\varepsilon_i \in N$). Since $q_1, q_2, \ldots, q_m$ are positive, pairwise coprime integers, we can hold that $q_1 \cdot \varepsilon_1 + q_2 \cdot \varepsilon_2 + \cdots + q_m \cdot \varepsilon_m = D_C$ by Lemma 3. Especially, we set $\varepsilon_1 = \varepsilon_2 = \cdots \varepsilon_m = 0$ when $D_C = 0$. Moreover, a minimal solution that minimizes the value of $(|\varepsilon_1| + |\varepsilon_2| + \cdots + |\varepsilon_m|)$ can be obtained easily by the extended Euclidean algorithm as stated previously in Bézout's Lemma. This lemma indicates that the minimal image distortion can be achieved by employing the minimal solution. In other words, the issue to embed the secret data b_i into the cover pixel p_i while minimizing the image distortion is feasible by the CRT-EMD scheme. □

3.2. The Embedding Process

Detailed description of the embedding process is provided in the following algorithm (Algorithm 4).

Algorithm 4 CRT-EMD Embedding Algorithm.

Input: cover image I_c and binary secret data stream S
Output: stego image I_s

Step 1. Divide the cover image I_c into non-overlapping m-pixel groups.
Step 2. Select m positive, pairwise coprime integers, $q_1, q_2, \ldots, q_m$, where $q_i \geq 2^{i+1}$ for $1 \leq i \leq m$.
Step 3. Obtain an m-pixel group $(p_1, p_2, \ldots, p_m)$ from I_c.
Step 4. For $i = 1$ to m do

Read $(i+1)$ secret bits from S;

Obtain the (2^{i+1})-ary value b_i of these bits.

End For.
Step 5. Compute $y = g_C(p_1, p_2, \ldots, p_m)$ by Equation (5).
Step 6. Compute an integer y' by CRT. First, establish Equation (6) by using $b_1, b_2, \ldots, b_m$ and $q_1, q_2, \ldots, q_m$. Finally, y' is computed by CRT as $y' = \sum_{i=1}^{m} M_i \cdot M_i' \cdot b_i \bmod \prod_{i=1}^{m} q_i$, where $M_i = \frac{\prod_{i=1}^{m} q_i}{q_i}$ and $M_i \cdot M_i' \equiv 1 (\bmod q_i)$.
Step 7. Compute the difference $D_C = (y' - y) \bmod \prod_{i=1}^{m} q_i$.
Step 8. Let the modification on p_i be ε_i ($\varepsilon_i \in N$) and find the minimal solution $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ for Equation (7).
Step 9. Compute the stego pixel $p_i' = p_i + \varepsilon_i$ for $1 \leq i \leq m$.
Step 10. Go to Step 3 until all secret data is embedded.

From the above embedding process, it can be observed that the CRT-EMD scheme has a very high embedding capacity since $(i+1)$ secret bits can be directly embedded into the ith cover pixel in a group. Now let us give a clear explanation for the embedding process of the CRT-EMD scheme.

Given two grayscale pixels $(43, 52)$ of a cover image and a binary secret data stream $S = (01100)_2$, we will show how to embed S into the above two-pixel group using CRT-EMD when $m = 2$. Because $m = 2$, the cover image is divided into non-overlapping groups for embedding, each contains 2 pixels. Accordingly, the binary secret stream S is divided into a 2-bit segment b_1 and 3-bit segment b_2, in which $b_1 = (01)_2 = 1$ and $b_2 = (100)_2 = 4$. Then, we select two coprime integers $q_1 = 5$ and $q_2 = 8$ and compute $y = g_C(p_1, p_2) = (p_1 \cdot q_1 + p_2 \cdot q_2) \bmod (q_1 \cdot q_2) = (43 \times 5 + 52 \times 8) \bmod (5 \times 8) = 31$ by Equation (5) (See Step 5). After that, we establish two equations $y' \bmod 5 = 1$ and $y' \bmod 8 = 4$ and compute $y' = 36$ by CRT. We then find the minimal solution $(\varepsilon_1 = 1, \varepsilon_2 = 0)$ for the equation $5 \cdot \varepsilon_1 + 8 \cdot \varepsilon_2 = D_C = (36 - 31) \bmod (5 \times 8) = 5$ according to Step 8. Thus, we obtain stego pixels $p_1' = p_1 + \varepsilon_1 = 43 + 1 = 44$ and $p_2' = p_2 + \varepsilon_2 = 52 + 0 = 52$.

3.3. The Extracting Process

Detailed steps of the extracting process are provided in the following algorithm (Algorithm 5).

Algorithm 5 CRT-EMD Extracting Algorithm.

Input: stego image I_s and a sequence of integers $q_1, q_2, \ldots, q_m$
Output: binary secret data stream S

Step 1. Divide the cover image I_s into non-overlapping m-pixel groups.
Step 2. Obtain an m-pixel group $(p_1', p_2', \ldots, p_m')$ from I_s.
Step 3. Compute $y' = g_C(p_1', p_2', \ldots, p_m')$ by Equation (5).
Step 4. Compute $b_i = y' \bmod q_i$ and convert b_i to $(i+1)$-bit binary data for $1 \leq i \leq m$.
Step 5. Go to Step 2 until all stego pixel groups have been processed. The binary secret data stream S is exactly retrieved by concatenating all binary data.

The extracting process implies that the extraction function constructed in the CRT-EMD scheme is different from those in previous EMD-type schemes. The secret data is computed directly by the

extraction function in existing schemes. In contrast, the value y' computed by the extraction function in Step 3 of CRT-EMD is not the embedded secret data but just an intermediate. Then, the secret data b_i is obtained by $b_i = y' \bmod q_i$. This two layer embedding strategy can further increase the security. To extract the hidden data in the stego pixel pair $(p'_1, p'_2) = (44, 52)$, we first compute $y' = g_C(p'_1, p'_2) = (44 \times 5 + 52 \times 8) \bmod (5 \times 8) = 36$, and then obtain secret data $b_1 = y' \bmod q_1 = 36 \bmod 5 = 1 = (01)_2$ and $b_2 = y' \bmod q_2 = 36 \bmod 8 = 4 = (100)_2$.

4. Experimental Results

In this section, the experimental results are given to evaluate the performance of the proposed scheme. Additionally, security analysis is given to demonstrate that the proposed scheme is immune to malicious attacks. All experiments are implemented by Matlab R2010A in a PC with an Intel(R) Core™ i7-4790 CPU @ 3.6 GHz and an 8-GB RAM. The operating system is Windows 7 Professional 64-bit.

4.1. Performance Evaluation

Since the performance evaluation of our proposed scheme depends on the embedding capacity and image quality, we will analyze them respectively and compare the results with previous schemes.

The embedding capacity (EC) of a data hiding scheme is defined as the number of secret bits that can be hidden in every cover pixel. Theorem 2 implies that our proposed scheme can achieve an extremely high embedding capacity.

Theorem 2. *The embedding capacity of the CRT-EMD data hiding scheme is at least 2.5 bpp (bits per pixel) and it increases when the number m of cover pixels in a group becomes larger.*

Proof. In the proposed CRT-EMD scheme, the cover pixel p_i in an m-pixel group can embed $(i+1)$ secret bits, so the embedding capacity is computed as

$$EC_{\text{CRT-EMD}} = (2 + 3 + \cdots + (m+1))/m = (m+3)/2 \text{ bpp}. \quad (14)$$

From Equation (14), we can infer that $EC_{\text{CRT-EMD}}$ increases when the size of cover pixel group increases and the minimal value of $EC_{\text{CRT-EMD}}$ is achieved at 2.5 bpp when there are two pixels in a group (i.e., $m = 2$). □

Figure 1 depicts the variation trend of embedding capacity of different schemes, including EMD [6], EMD-2 [10], GEMD [16], Sun et al.'s scheme [15], MSD [17], BPEMD [18] and the proposed CRT-EMD scheme. From Figure 1, we can observe that the maximum embedding capacity of EMD is 1.16 bpp when $m = 2$ and the embedding capacity decreases drastically if the size of pixel group increases. The embedding capacity of EMD-2 is a little bit better than EMD but still decreases dramatically when m increases as EMD did. On the contrary, the embedding capacity of GEMD, MSD, BPEMD and Sun et al.'s scheme can always maintain more than 1 bpp in spite of what value of m is. In particular, the embedding capacity of Sun et al.'s scheme always approaches 1.6 bpp; the best embedding capacity of both GEMD and BPEMD is 1.5 bpp, which is better than that of MSD under the same condition of $m = 2$. Compared to the aforementioned data hiding schemes, the proposed CRT-EMD scheme can significantly increase the embedding capacity in such a way that the embedding capacity can maintain at least 2.5 bpp and it increases when the number of cover pixels in a group increases.

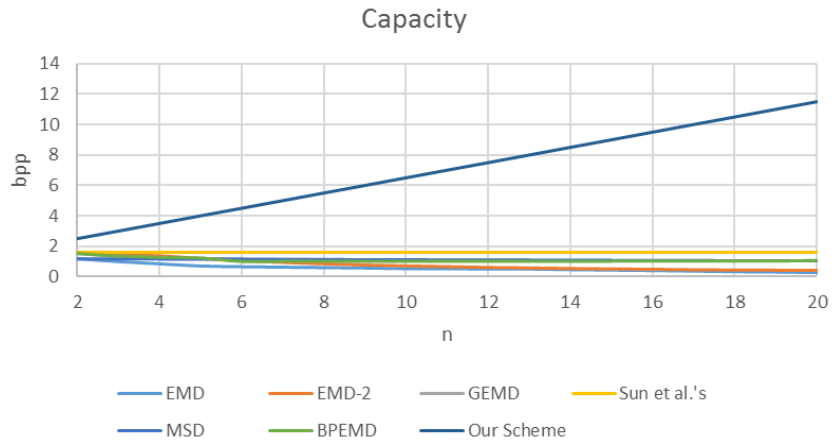

Figure 1. Comparison of embedding capacity. EMD: exploiting modification direction; GEMD: generalized EMD; MSD: modified signed digit; BPEMD: binary power EMD.

Next, we investigate the image quality of our proposed scheme. In our experiments, ten 512×512 grayscale images, i.e., Baboon, Airplane, Fishing boat, Girl, Gold hill, Lena, Peppers, Sailboat, Tiffany and Toys are used as the cover images. To evaluate the image quality, the peak signal to noise ratio (PSNR) is used and defined as follows:

$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right), \tag{15}$$

where the mean square error (MSE) for a $W \times H$ grayscale image is defined as follows:

$$\mathrm{MSE} = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(x_{ij} - x'_{ij}\right)^2, \tag{16}$$

where x_{ij} and x'_{ij} are the cover pixel value and the stego pixel value at location (i, j), respectively. As can be seen from Equation (15), a smaller MSE can lead to a larger PSNR which indicates that the stego image is more similar to the original cover image.

Figure 2 illustrates the stego images produced by our proposed scheme when $m = 2$. Figure 2a,c,e,g,i,k,m,o,q,s is the original cover images, and Figure 2b,d,f,h,j,l,n,p,r,t is the stego images. It is can be observed that the image quality is not degraded by our proposed scheme even if there is a large amount of data embedded in the cover image.

To thoroughly evaluate the performance of the proposed scheme, Tables 1 and 2 compare the proposed scheme with four previous schemes [6,16–18] in terms of payload and image quality under $m = 2$ and $m = 3$, respectively. In both tables, "Payload (bits)" represents the total number of secret bits embedded in a 512×512 grayscale cover image and "PSNR (dB)" represents the visual quality of the stego image after embedding. It can be implied from Table 1 that the payload for $m = 2$ of the proposed scheme is significantly better than that of others, meanwhile PSNR value is greater than 41 dB. More specifically, the payload of the proposed scheme is about 262,144 to 340,788 bits larger than that of others, especially twice larger than that of EMD and MSD. On the other hand, the payload for $m = 3$ of the proposed scheme increases to 785,920 bits as shown in Table 2, making the payload difference between the proposed scheme and other schemes even larger, achieving at least 445,133 bits. Fortunately, PSNR value of the proposed scheme still maintains greater than 32 dB when $m = 3$, which indicates that the distortion of the stego image cannot be detected by human eyes.

Figure 2. Ten 512 × 512 grayscale cover images and their stego-images. (**a**) Original image, Baboon; (**b**) Stego-image, Baboon; (**c**) Original image, Airplane; (**d**) Stego-image, Airplane; (**e**) Original image, Fishingboat; (**f**) Stego-image, Fishingboat; (**g**) Original image, Girl; (**h**) Stego-image, Girl; (**i**) Original image, Goldhill; (**j**) Stego-image, Goldhill; (**k**) Original image, Lena; (**l**) Stego-image, Lena; (**m**) Original image, Peppers; (**n**) Stego-image, Peppers; (**o**) Original image, Sailboat; (**p**) Stego-image, Sailboat; (**q**) Original image, Tiffany; (**r**) Stego-image, Tiffany; (**s**) Original image, Toys; (**t**) Stego-image, Toys.

Table 1. Performance comparisons under $m = 2$. **PSNR:** peak signal to noise ratio.

$m = 2$	EMD [6]		GEMD [16]		MSD [17]		BPEMD [18]		Our Scheme	
	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR
Baboon	314,572	52.10	393,216	50.20	314,572	52.11	393,216	49.39	655,360	41.61
Airplane	314,572	52.10	393,216	50.16	314,572	52.11	393,216	49.43	655,360	41.63
Fishing boat	314,572	52.10	393,216	50.23	314,572	52.11	393,216	49.41	655,360	41.62
Girl	314,572	52.10	393,216	50.22	314,572	52.11	393,216	49.44	655,360	41.62
Gold hill	314,572	52.10	393,216	50.17	314,572	52.11	393,216	49.37	655,360	41.64
Lena	314,572	52.10	393,216	50.19	314,572	52.11	393,216	49.43	655,360	41.63
Peppers	314,572	52.10	393,216	50.23	314,572	52.11	393,216	49.36	655,360	4159
Sailboat	314,572	52.10	393,216	50.24	314,572	52.11	393,216	49.39	655,360	41.56
Tiffany	314,572	52.10	393,216	50.22	314,572	52.11	393,216	49.41	655,360	41.60
Toys	314,572	52.10	393,216	50.18	314,572	52.11	393,216	49.36	655,360	41.58

Table 2. Performance comparisons under $m = 3$.

$m = 3$	EMD [6]		GEMD [16]		MSD [17]		BPEMD [18]		Our Scheme	
	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR
Baboon	235,929	53.56	340,787	50.82	317,194	51.90	340,787	50.49	785,920	32.51
Airplane	235,929	53.61	340,787	50.84	317,194	51.90	340,787	50.46	785,920	32.50
Fishing boat	235,929	53.67	340,787	50.81	317,194	51.90	340,787	50.47	785,920	32.49
Girl	235,929	53.59	340,787	50.80	317,194	51.90	340,787	50.45	785,920	32.45
Gold hill	235,929	53.54	340,787	50.78	317,194	51.90	340,787	50.49	785,920	32.51
Lena	235,929	53.58	340,787	50.77	317,194	51.90	340,787	50.47	785,920	32.51
Peppers	235,929	53.68	340,787	50.83	317,194	51.90	340,787	50.43	785,920	32.59
Sailboat	235,929	53.63	340,787	50.75	317,194	51.90	340,787	50.47	785,920	32.53
Tiffany	235,929	53.61	340,787	50.81	317,194	51.90	340,787	50.46	785,920	32.49
Toys	235,929	53.51	340,787	50.81	317,194	51.90	340,787	50.45	785,920	32.53

Based on the above analyses, the proposed scheme outweighs other related schemes since it can embed much more secret data into a cover image without any visual perception. Moreover, the proposed scheme can achieve very good balance between the payload and the image quality under different values of m, so that we can adjust m to meet different requirements. For instance, the proposed scheme for $m = 2$ will be employed if better image quality is required and for $m = 3$ will be used if higher payload is needed. In future work, we will focus on the combination of situations for different m to achieve a better balance between the payload and the image quality.

4.2. Security Analysis

In this subsection, we first theoretically demonstrate the security of the proposed scheme, and then analyze that the proposed scheme can withstand visual attacks [3]. Two analysis approaches of visual attacks, i.e., bit plane attack [18] and enhancing LSBs attack [12] are applied to evaluate the security of the proposed scheme.

The number of pixels change rate (NPCR) is used as a criterion to measure the security in theory. NPCR is the percentage of different pixel numbers between the cover image and the stego image, which is defined as follows:

$$\mathrm{NPCR}(I_c, I_s) = \frac{\sum_{i,j} A(i,j)}{W \times H} \times 100\%, \tag{17}$$

where W and H represent the width and the height of the cover image I_c and stego image I_s while $A(i,j)$ is computed as:

$$A(i,j) = \begin{cases} 1, & x_{ij} \neq x'_{ij} \\ 0 & x_{ij} = x'_{ij} \end{cases}. \tag{18}$$

The expected NPCR value is 99.61% for a grayscale image. Table 3 lists the NPCR values for the proposed scheme and the average NPCR is about 86.13% for $m = 2$ and 84.82% for $m = 3$, which are very close to the expected value. This provides a strong evidence to ensure that our scheme is secure theoretically.

Table 3. Number of pixels change rate (NPCR) values of the proposed scheme.

Image	Our Scheme	
	NPCR ($m = 2$)	NPCR ($m = 3$)
Baboon	86.04%	84.79%
Airplane	86.10%	84.87%
Fishing boat	86.12%	84.80%
Girl	86.26%	85.02%
Gold hill	86.27%	84.91%
Lena	86.11%	84.93%
Peppers	86.07%	83.73%
Sailboat	86.11%	84.90%
Tiffany	86.09%	84.81%
Toys	86.08%	84.43%
Average	86.13%	84.82%

In the bit plane attack [18], a plane image is constructed by extracting corresponding bit of each pixel in the original image. The 512 × 512 8-bit grayscale cover image "Baboon" and its stego image are used in our experiment to conduct the bit plane attack. Eight plane images for the cover image and the corresponding stego image ($m = 3$) are shown in Figures 3 and 4, respectively. Results reveal that a malicious attacker is unable to find any clues to embedded secret data by investigating Figures 3 and 4 because the modification on each cover pixel has no direct relationship with secret data. Thus, the proposed scheme is secure against the bit plane attack.

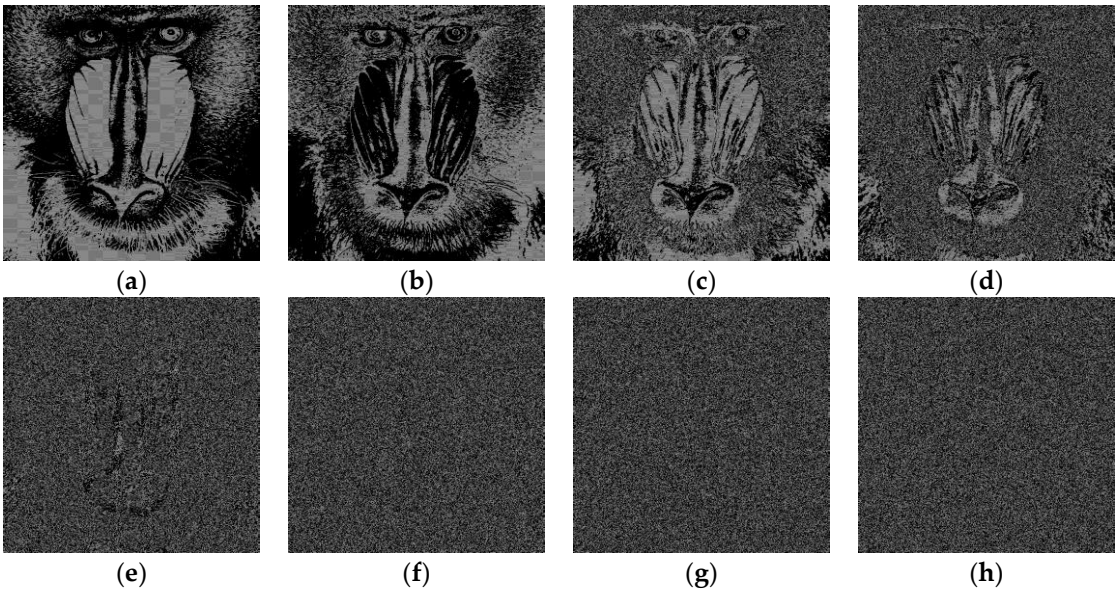

Figure 3. Plane images of 512 × 512 cover image "Baboon". (**a**) 8th bit; (**b**) 7th bit; (**c**) 6th bit; (**d**) 5th bit; (**e**) 4th bit; (**f**) 3rd bit; (**g**) 2nd bit; (**h**) 1st bit.

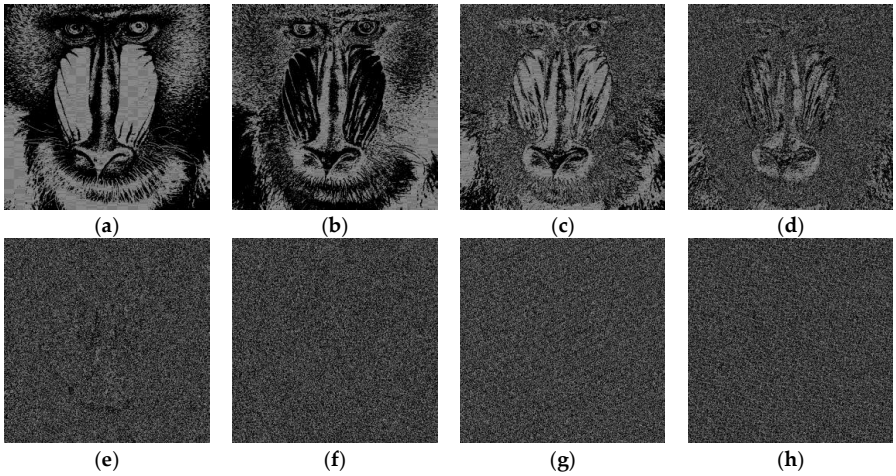

Figure 4. Plane images of 512 × 512 stego image of "Baboon". (**a**) 8th bit; (**b**) 7th bit; (**c**) 6th bit; (**d**) 5th bit; (**e**) 4th bit; (**f**) 3rd bit; (**g**) 2nd bit; (**h**) 1st bit.

In the enhancing LSBs attack [12], a pattern image is generated by extracting k LSBs of each pixel of the original grayscale image and then making them most-significant bits (MSBs) followed by a sequence of "0" bits with length of $(8-k)$. If a stego-image is produced by LSB substitution, a specific pattern will appear in the pattern image so that the attacker can detect the use of LSB. In our experiment, we perform the enhancing LSBs attack ($k = 3$) on two stego images, one (see Figure 5a) is produced by LSB substitution and the other (see Figure 5c) by our proposed scheme. Obviously, Figure 5b shows that there is a specific pattern for LSB substitution when the enhancing LSBs attack is launched on Figure 5a. On the contrary, the proposed scheme embeds the secret data according to the CRT and an extraction function rather than using LSB substitution, so no specific pattern is determined (see Figure 5d). Finally, Table 4 summarizes the features of typical EMD-type data hiding schemes.

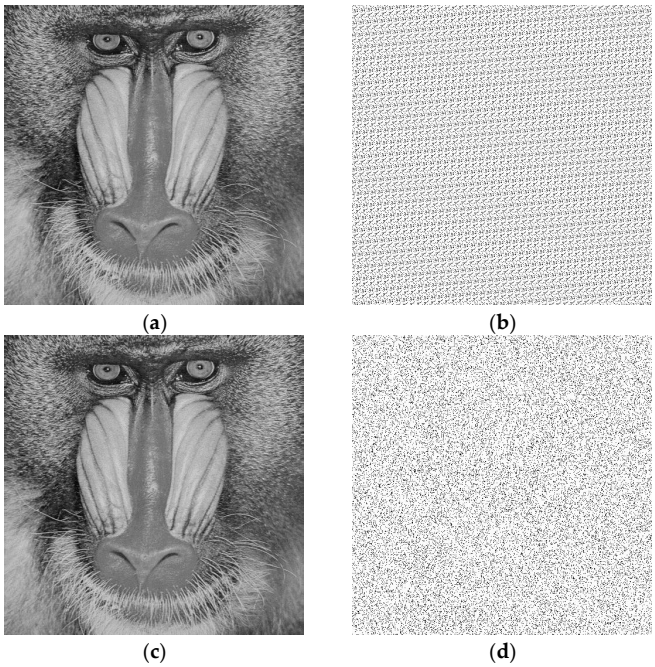

Figure 5. The enhancing least-significant bits (LSBs) attack for "Baboon". (**a**) Stego-image embedded by LSB; (**b**) Enhancing LSBs attack on (**a**); (**c**) Stego-image embedded by our proposed scheme; (**d**) Enhancing LSBs attack on (**c**).

Table 4. Comparisons of features of EMD-type schemes.

Feature	EMD [6]	GEMD [16]	MSD [17]	BPEMD [18]	Our Scheme
Binary secret data embedded directly	No	Yes	No	Yes	Yes
Maximum embedding capacity (bpp)	1.16	1.5	1.16	1.5	$\geq$2.5
Good PSNR (>30 dB)	Yes	Yes	Yes	Yes	Yes
Coefficient and modulus are 2-power	No	No	No	Yes	No

5. Conclusions

In this paper, we proposed a high capacity EMD-type data hiding scheme based on CRT. To the best of our knowledge, it is the first EMD-type scheme that uses CRT as its main building block. In the proposed scheme, a novel extraction function is constructed in which the coefficients are pairwise coprime integers and the modulus is the product of the coefficients. According to the CRT and the constructed extraction function, the cover image is divided into non-overlapping m-pixel groups and the ith cover pixel in a group can directly embed as much as $(i+1)$ secret bits. The embedding capacity of the proposed scheme is significantly high while guaranteeing good image quality. In particular, the embedding capacity can maintain at least 2.5 bpp and increase when the number of cover pixels in a group increases. Experimental results showed that the proposed scheme, in comparison with some related schemes, outperforms in achieving a better balance between the embedding capacity and the image quality.

Author Contributions: Yanjun Liu and Chin-Chen Chang proposed the idea of the paper; Yanjun Liu wrote the paper; Peng-Cheng Huang conceived and designed the experiments; Cheng-Yi Hsu performed the experiments.

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

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Turner, L. Digital data security system. *Patent IPN wo* **1989**, *89*, 08915.
3. Westfeld, A.; Pfitzmann, A. *Attacks on Steganographic Systems, International Workshop on Information Hiding*; Springer: Berlin, Germany, 1999; pp. 61–76.
4. Ker, A.D. *Improved Detection of Lsb Steganography in Grayscale Images, International Workshop on Information Hiding*; Springer: Berlin, Germany, 2004; pp. 97–115.
5. Mielikainen, J. LSB matching revisited. *IEEE Signal Process. Lett.* **2006**, *13*, 285–287. [CrossRef]
6. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
7. Lee, C.F.; Chang, C.C.; Wang, K.H. An improvement of emd embedding method for large payloads by pixel segmentation strategy. *Image Vis. Comput.* **2008**, *26*, 1670–1676. [CrossRef]
8. Chang, C.C.; Chou, Y.C.; Kieu, T.D. An information hiding scheme using sudoku. In Proceedings of the ICICIC'08 3rd International Conference on Innovative Computing Information and Control, Dalian, China, 18–20 June 2008; pp. 17–22.
9. Hong, W.; Chen, T.S.; Shiu, C.W. A minimal euclidean distance searching technique for sudoku steganography. In Proceedings of the ISISE'08 International Symposium on Information Science and Engineering, Shanghai, China, 20–22 December 2008; pp. 515–518.
10. Kim, H.; Kim, C.; Choi, Y.; Wang, S.; Zhang, X. Improved modification direction methods. *Comput. Math. Appl.* **2010**, *60*, 319–325. [CrossRef]
11. Chang, C.C.; Liu, Y.; Nguyen, T.S. A novel turtle shell based scheme for data hiding. In Proceedings of the 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Kitakyushu, Japan, 27–29 August 2014; pp. 89–93.
12. Liu, Y.; Chang, C.C.; Nguyen, T.S. High capacity turtle shell-based data hiding. *IET Image Process.* **2016**, *10*, 130–137. [CrossRef]

13. Kieu, T.D.; Chang, C.C. A steganographic scheme by fully exploiting modification directions. *Expert Syst. Appl.* **2011**, *38*, 10648–10657. [CrossRef]
14. Shen, S.Y.; Huang, L.H. A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Comput. Secur.* **2015**, *48*, 131–141. [CrossRef]
15. Sun, H.M.; Weng, C.Y.; Wang, S.J.; Yang, C.H. Data embedding in image-media using weight-function on modulo operations. *ACM Trans. Embed. Comput. Syst.* **2013**, *12*, 21. [CrossRef]
16. Kuo, W.C.; Wang, C.C. Data hiding based on generalised exploiting modification direction method. *Imaging Sci. J.* **2013**, *61*, 484–490. [CrossRef]
17. Kuo, W.C.; Wang, C.C.; Hou, H.C. Signed digit data hiding scheme. *Inf. Process. Lett.* **2016**, *116*, 183–191. [CrossRef]
18. Kuo, W.C.; Wang, C.C.; Huang, Y.C. Binary power data hiding scheme. *AEU Int. J. Electr. Commun.* **2015**, *69*, 1574–1581. [CrossRef]
19. Zhang, X.; Long, J.; Wang, Z.; Cheng, H. Lossless and reversible data hiding in encrypted images with public-key cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 1622–1631. [CrossRef]
20. Cao, X.; Du, L.; Wei, X.; Meng, D.; Guo, X. High capacity reversible data hiding in encrypted images by patch-level sparse representation. *IEEE Trans. Cybern.* **2016**, *46*, 1132–1143. [CrossRef] [PubMed]
21. Qian, Z.; Zhang, X. Reversible data hiding in encrypted images with distributed source encoding. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 636–646. [CrossRef]
22. Harn, L.; Miao, F.; Chang, C.C. Verifiable secret sharing based on the chinese remainder theorem. *Secur. Commun. Netw.* **2014**, *7*, 950–957. [CrossRef]
23. Chang, C.C.; Huynh, N.T.; Le, H.D. Lossless and unlimited multi-image sharing based on chinese remainder theorem and lagrange interpolation. *Signal Process.* **2014**, *99*, 159–170. [CrossRef]
24. Liu, Y.; Harn, L.; Chang, C.C. A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets. *Int. J. Commun. Syst.* **2015**, *28*, 1282–1292. [CrossRef]
25. Tignol, J.P. *Galois' Theory of Algebraic Equations*; World Scientific: Singapore, 2001.