symmetry

MDPI

Article

Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images

Mehdi Hussain [1,2], Ainuddin Wahid Abdul Wahab [1,*], Noman Javed [3] and Ki-Hyun Jung [4,*]

1 Department of Computer System & Technology, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia; mehdi141@siswa.um.edu.my
2 School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad 44000, Pakistan
3 Department of Computer Science, Namal College (an Associate College of the University of Bradford, UK), Mianwali 42250, Pakistan; noman.javed@namal.edu.pk
4 Department of Cyber Security, Kyungil University, 712-701, Korea
* Correspondence: ainuddin@um.edu.my (A.W.A.W.); khanny.jung@gmail.com (K.-H.J.); Tel.: +60-3-79676383 (A.W.A.W.); +82-53-600-5626 (K.-H.J.)

Academic Editor: Sergei Odintsov
Received: 3 February 2016; Accepted: 23 May 2016; Published: 31 May 2016

Abstract: The goal of image steganographic methods considers three main key issues: high embedding capacity, good visual symmetry/quality, and security. In this paper, a hybrid data hiding method combining the right-most digit replacement (RMDR) with an adaptive least significant bit (ALSB) is proposed to provide not only high embedding capacity but also maintain a good visual symmetry. The cover-image is divided into lower texture (symmetry patterns) and higher texture (asymmetry patterns) areas and these textures determine the selection of RMDR and ALSB methods, respectively, according to pixel symmetry. This paper has three major contributions. First, the proposed hybrid method enhanced the embedding capacity due to efficient ALSB utilization in the higher texture areas of cover images. Second, the proposed hybrid method maintains the high visual quality because RMDR has the closest selection process to generate the symmetry between stego and cover pixels. Finally, the proposed hybrid method is secure against statistical regular or singular (RS) steganalysis and pixel difference histogram steganalysis because RMDR is capable of evading the risk of RS detection attacks due to pixel digits replacement instead of bits. Extensive experimental tests (over 1500+ cover images) are conducted with recent least significant bit (LSB)-based hybrid methods and it is demonstrated that the proposed hybrid method has a high embedding capacity (800,019 bits) while maintaining good visual symmetry (39.00% peak signal-to-noise ratio (PSNR)).

Keywords: information hiding; hybrid steganography; image security; right-most digit replacement; visual symmetry

1. Introduction

Internet evolution has led to the rapid transmission of digital content such as images, audio, text, and videos. Meanwhile, advancement of forgery tools and applications means that digital content can easily be altered, copied, and destroyed during transmission. In order to secure the transmission of data and prevent its manipulation, a security system provides two main disciplines: information encryption and information hiding (see Figure 1). Information encryption, or cryptography, is a process of transforming the data using a crypto-key so it becomes unintelligent. There are different client/server architectures [1,2] based applications employed the encryption algorithms to secure its data during transmission. On the other hand, information hiding is the art and science of hiding

secret data such that its presence cannot be detected [3]. Information hiding can be further classified into watermarking and steganography (see Figure 1). Watermarking protects intellectual copyright and guarantees the integrity of transmitted data. In general, watermarking is useful for small sizes of information such as a company's logo or author's tags [3]. Steganography is the art of using the communication medium in such a way that it conceals the existence of secret data [3,4]. The communication medium can be image, text, audio, or video.

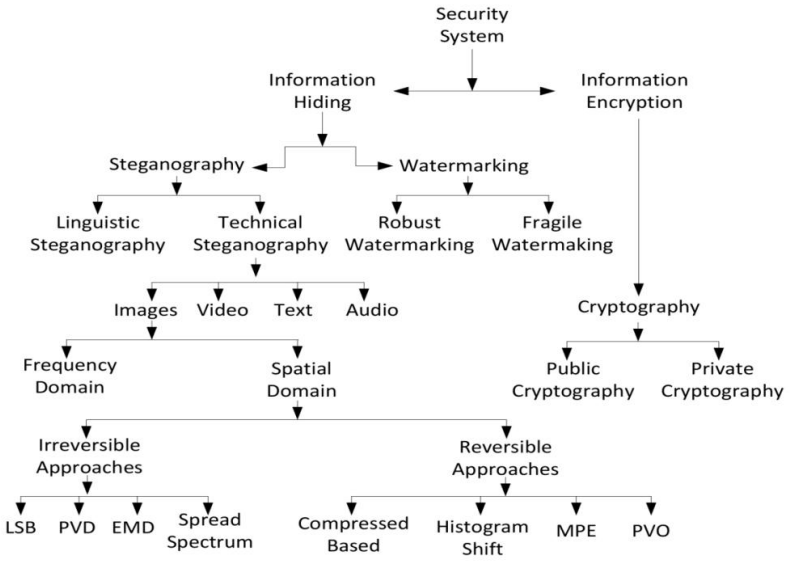


Figure 1. General classification of information hiding systems.

Generally, the image steganographic method is evaluated by three key perspectives: capacity (the maximum payload that could be embedded into the cover-image), visual symmetry (the stego-image should be perceptually identical to its cover-image), and security (the stego-image must be resistant to steganalysis detection attacks). Hence, the ideal steganographic method should be simultaneously capable of high capacity, good visual symmetry, and undetectability. Most often, high payload steganographic methods introduce the distortion artifacts in stego-images and are vulnerable to steganalysis. Moreover, good visual quality steganographic methods suffer from the low payload. How to simultaneously achieve high capacity, visual symmetry, and security is a challenging research problem due to the contradictions between them.

Numerous image steganography methods are available in the literature. These methods are categorized into two major divisions, spatial and frequency domains. In the spatial domain, the secret data is embedded directly by modifying the pixel intensities, whereby, in the frequency domain, the information is embedded into the transformed coefficient of cover images. The frequency domain methods are more robust against detection attacks as compared to the spatial domain, but they have low payloads and are computationally expensive [5]. Conversely, the high payload, good visual quality, and low computational cost of the spatial domain make it useful for image steganography, so the proposed work carried out in this paper is based on the spatial domain.

Recently, data embedding applications have divided steganographic methods into reversible and irreversible approaches. The reversible steganographic methods reconstruct the original image after extracting the secret message from the stego-images. Such embedding approaches suffer from low payload as compared to irreversible methods. To increase the embedding capacity of reversible approaches, data compression methods are applied to the secret message before the embedding process [6,7]. In contrast, irreversible steganography attempts to achieve a high embedding payload and good visual symmetry without giving much attention to recovering the cover-image during the extraction process.

The fundamental and common irreversible image steganographic method is least significant bit (LSB) substitution [8]. It replaces bits of pixels to hide the secret data. In LSB-based methods, the payload is dependent on the utilization of least bit substitution; it directly affects the visual quality of stego-images. Optimal pixel adjustment process (OPAP) [9] was applied to LSB-based pixels to improve the visual quality of stego-image. Although LSB-based methods are efficient, due to asymmetry structures they can easily be exposed by statistical steganalysis detection attacks [10–12]. On the other hand, LSB matching (LSBM), also known as ± 1 embedding, can solve or avoid the asymmetric structure of the LSB replacement method. Generally, in LSBM, if the secret bit does not match the LSB of the cover pixel, then a random ± 1 is added to the cover pixel value. However, LSB matching does not lead to the asymmetric changes in the pixels. Consequently, it is more difficult to detect LSB matching than LSB replacement [12]. Furthermore, LSBM-based methods can be utilized to achieve n bpp secret data embedding [13].

With respect to undetectability, generally, modern steganographic methods prioritize high security instead of high payload or visual quality of stego-images. Therefore, the state-of-the-art highly undetectable stego (HUGO) [14] method is proposed based on the LSB matching algorithm. It consists of a high dimensional image model to calculate the distortions corresponding to a modification of each pixel by ± 1, but can only hide up to 1 bpp. Similarly, wavelet obtained weights (WOW) [15], spatial universal wavelet relative distortion (S-UNIWARD) [16], HIgh Low Low (HILL) [17], and minimizing the power of optimal detector (MiPOD) [18] are targeted as highly secure steganographic methods with limited payload.

On the other hand, classical steganographic methods provide higher payload, usually more than 1 bpp. Wu and Tsai proposed a pixel value difference (PVD) method that embeds the secret data by readjusting the difference between two consecutive pixels and has a good visual symmetry [19]. In the literature, PVD-based methods considered different directions of pixels' differences, along with human vision system (HVS) smoothness and edginess sensitivity, to determine the number of secret bits for embedding [20,21]. In general, PVD-based methods improved the visual quality; however, the difference histogram of stego-images deviated from the cover-image and was vulnerable to histogram analysis. Zhang and Wang introduced an exploiting modification direction (EMD) for data hiding, where n number of pixels were utilized to hide the $(2n + 1)$ base secret digits [22]. Furthermore, different EMD-based methods [23–26] were proposed to improve the visual quality but suffered from low payload.

Researchers have also combined different singular steganographic techniques into hybrid data embedding methods. Generally, hybrid embedding methods utilized the advantages of existing singular steganographic approaches; for example, high payload of LSB and good imperceptibility of PVD methods are employed in [27–31]. Furthermore, the hybrid steganographic methods are more secure, because many steganalysis detection attacks are specifically designed to target a singular steganography method [10–12,32]. Thus hybrid embedding approaches generally confuse the statistical steganalysis methods used to detect the stego-images [33].

Wu *et al.* [27] proposed a hybrid embedding method based on LSB and PVD approaches. It divided the cover-image into edginess and smoothness levels; further, the LSB and PVD methods were applied on smooth and edge areas, respectively. Regardless of the fact that this method improved the payload and visual quality, it failed to resist RS-analysis detection attacks [10]. In [29,31], Jung proposed methods to combine LSB with multi-pixel differencing and PVD with modulus function. These methods improved hidden capacity and retained acceptable visual quality but suffered from low security. Yang *et al.* [34] enhanced Wu *et al.*'s [27] method by introducing a lower level readjustment strategy. This method improved visual quality and undetectability against RS detection attacks. However, the limitation of this method is that the pixel difference showed asymmetrical curves in the histogram. To obtain high payload and good visual quality, Khodaei *et al.* [28] combined the k-bit LSB with the PVD method. This method divided the pixels into three non-overlapping pixel blocks. The k-bit LSB method was applied to the base/center pixel and PVD was applied to the other two

pixels of the block. Tsai *et al.* [30] enhanced the Khodaei *et al.* [28] method by introducing an adaptive $m \times n$ pixel blocks for selection of edge regions in the cover-image to increase the payload. However, this method reduced the visual quality of the stego-image. To obtain good visual quality and high payload, Hsiao Shan [35] proposed a multi-way PVD method by combining the tri-way PVD and mode selection process, while this combination improved the visual quality but has low payload as compared to [28]. Shen *et al.* suggested a reversible data embedding method by combining the PVD with modulus function for color images, thus having a low payload [36]. Moreover, Shen *et al.* [26] proposed another method with high capacity and good visual imperceptibility compared to that of Zhang and Wang [22]. This method combined the PVD and EMD methods and suffers from low payload as compared with the latest hybrid embedding methods [25,27–29,34]. Recently, Wu *et al.* [25] proposed a hybrid method for high payload and good visual quality by combining LSB, EMD, and modification of prediction errors (MPE) methods. This method provided two adaptive solutions for steganographic applications; the first solution targeted the good visual quality and the second solution is high hidden capacity. As we observed through experiments, Wu *et al.* [25] obtained a lower payload as compared with existing hybrid methods. Furthermore, this method is exposed by pixel difference histogram analysis (see Section 3.5).

It is observed that the aforementioned hybrid methods provide good payload and acceptable visual quality [37] in stego-images. However, all of the aforementioned methods can easily be exposed to state-of-the-art ensemble-based subtractive pixel adjacency matrix (SPAM) steganalysis methods [38]. This indicates that these methods are more concerned with the payload and visual quality than they are with undetectability. This is in spite of the fact that some of them are unable to provide a competent payload [25,27–29,31,34,35], and do not fully utilize the advantages of singular steganographic methods [25,27–29,34]. Furthermore, existing hybrid methods are unable to achieve simultaneous high payload, good visual quality, and undetectability (at least lower bpp) in one steganographic solution.

Motivated by the above facts, our main goal is to propose a hybrid steganographic method, which provides a high embedding capacity while maintaining good visual symmetry and structural undetectability against RS and difference histogram steganalysis. The paper contributions are as follows. First, we propose a novel singular steganographic right-most digit replacement (RMDR) method to provide 3 bpp for lower texture areas with improved visual quality. Second, we utilize the adaptive k-bit LSB OPAP [9] as an adaptive least significant bit (ALSB) method to improve hidden capacity for higher texture areas. Furthermore, we combine ALSB with RMDR into one steganographic approach to create a hybrid method that maintains the advantages of both (high payload and good visual quality).

The organization of the paper is as follows. This section discussed related work on LSB-based hybrid steganographic approaches. Section 2 proposes a hybrid steganographic method, with details of embedding and extraction procedures. In Section 3, detailed experimental results are presented and discussed. Conclusions and future directions are presented in Section 4.

2. Proposed Hybrid Data Embedding Method

In this section, we present a hybrid data embedding scheme. This hybrid method is based on two steganographic approaches, RMDR and ALSB [9]. RMDR is a novel proposed method for high visual quality and undetectability, while ALSB [9] is utilized to achieve high payload. In proposed hybrid embedding, the selection of k-bit ALSB with RMDR is inspired by following methods [25,27,34].

In the proposed scheme, the cover-image is divided into two regions inspired by [27] *i.e.*, region-1 and region-2 for lower and higher texture areas, respectively, as shown in Table 1. Further, these texture regions are categorized into four *Rn* difference ranges based on the width, where $n = 4$, e.g., R_1 [0, 31] to R_4 [128, 255]. On the other hand, the second row of Table 1 shows the pre-estimated number of secret bits for embedding in each pixel. For example, the R_1 range exists under region-1 and 3-bits secret data are used to embed in each pixel. Furthermore, these ranges can be dynamically generated depending

on the steganographic requirement. For experiments, we propose the following regions and ranges of Table 1, which meet the proposed method goals, *i.e.*, high payload and acceptable visual quality.

Table 1. Proposed hybrid embedding method range table divisions as region-1 and region-2 levels, where k denotes the least bits for embedding.

Regions	Region-1 Level	Region-2 Level		
Lower-Upper bound of R_n	$R_1 \in [0, 31]$	$R_2 \in [32, 63]$	$R_3 \in [64, 127]$	$R_4 \in [128, 255]$
Secret bits	3	$k = 4 = \log_2(63 - 32) - 1$	$k = 5 = \log_2(127 - 64) - 1$	$k = 6 = \log_2(225 - 128) - 1$

The complete description of the proposed RMDR embedding and hybrid embedding methods are presented in Sections 2.1 and 2.2. In addition, both proposed extraction parts of the above RMDR and hybrid methods are presented in Sections 2.3 and 2.4.

2.1. RMDR Embedding Method

In the RMDR embedding process, the right-most digit of a pixel value is utilized for embedding the secret data, so a decomposition of the pixel value is required to separate the pixel digits. For this reason, a pixel value is decomposed into three digit levels. For example, a pixel value $g \in [0, 255]$ and its proposed decomposition of digit levels are denoted as left digit (*LD*), middle digit (*MD*), and right digit (*RD*), as described in Equation (1), where *LD* range $\in [0, 2]$, *MD* and *RD* ranges $\in [0, 9]$. For example, if $g = 243$, its *LD*, *MD*, and *RD* decomposed values are 2, 4, and 3, respectively. If a pixel value consists of only one/two digit(s) then a leading zero(s) is added to occupy the *LD* or *MD*, such as $g = 4$ where *LD* and *MD* are 0 and *RD* is 4.

$$g = (100 \times LD + 10 \times MD + 1 \times RD) \quad (1)$$

In the embedding process, the three secret bits are converted into stegoRD from Table 2. Table 2 consists of three columns, namely b, $SRD_0(b)$ and $SRD_1(b)$, where b is a three-bit secret decimal data, and $SRD_0(b)$ and $SRD_1(b)$ are the stegoRDs (mapped RDs) against b. In our experiments, the generation of mapping table (Table 2) is as follows: the three-bit secret digit, 2^3 range is [0, 7], and a pixel *RD* range is [0, 9]. The pixel *RD* range has two extra digits as {8, 9} that can be reused with three-bit secret digits as replacing with {3, 4} digit value. These two extra digits aim at minimizing the difference between cover and stego-pixels RDs. Alternatively, it can be adaptively generated by considering the frequency of RDs in cover images.

Table 2. StegoRD decimal digit values mapping table for the RMDR embedding method.

b	$SRD_0(b)$	$SRD_1(b)$
0	0	−1
1	1	−1
2	2	−1
3	3	8
4	4	9
5	5	−1
6	6	−1
7	7	−1

In the RMDR embedding method, two cover pixels (g_i, g_{i+1}) considered as a block (i) are utilized to hide the secret data. The six secret bits are divided and converted into two three-bit decimals; their equivalent stegoRD ($SRD_0(b)$ and $SRD_1(b)$) values are derived from Table 2. Furthermore, the best nearest stego-pixels values are calculated with their stegoRDs. Finally, the resultant stego-block difference must exist in region-1 of Table 1. The detailed embedding steps with examples are described in Scheme 1.

Let	g_i *and* g_{i+1} *are the* ***i****th block pixels values of C,* ***M*** *be the secret message bits streams. In Table 2, b refers to both* b_i *and* b_{i+1} *For* $SRD_0(b)$ *and* $SRD_1(b)$ *are stego-right-digits (stegoRD), refers to* $SRD_{0(b_i)}$, $SRD_{0(b_{i+1})}$ *and* $SRD_{1(b_i)}$, $SRD_{1(b_{i+1})}$ *respectively.*	
Begin:		
	Step 1	***Read*** $n = 6$ (n_5, n_4, n_3, n_2, n_1, n_0) *bits from M,* ***generate*** *two decimals as* $b_i = (n_5 n_4 n_3)_{10}$ *and* $b_{i+1} = (n_2 n_1 n_0)_{10}$.
	Step 2	***Find*** *the respective* $SRD_{0(b_i)}$, $SRD_{1(b_i)}$ *against* b_i *and* $SRD_{0(b_{i+1})}$, $SRD_{1(b_{i+1})}$ *for* b_{i+1} *(from Table 2).*
	Step 3	***Discard*** *the* $SRD_{1(b_i)}$ *and* $SRD_{1(b_{i+1})}$ *in case of −1.*
	Step 4	***Generate*** *the nearest pixels (high, medium and low values) against* g_i *using Equation (2) where its RDs must be matched either with* $SRD_{0(b_i)}$ *or* $SRD_{1(b_i)}$ *for* b_i *case, denoted as* S_0g_{iH}, S_0g_{iM}, S_0g_{iL}, S_1g_{iH}, S_1g_{iM}, S_1g_{iL} *and* $\in$ *[0, 255].* $$\begin{aligned} S_0g_{iL} &= NearPixFun\left(g_i - 10\,,\, SRD_{0(b_i)}\right) & S_1g_{iL} &= NearPixFun\left(g_i - 10\,,\, SRD_{1(b_i)}\right) \\ S_0g_{iM} &= NearPixFun\left(g_i\,,\, SRD_{0(b_i)}\right) & S_1g_{iM} &= NearPixFun\left(g_i\,,\, SRD_{1(b_i)}\right) \\ S_0g_{iH} &= NearPixFun\left(g_i + 10\,,\, SRD_{0(b_i)}\right), & S_1g_{iH} &= NearPixFun\left(g_i + 10\,,\, SRD_{1(b_i)}\right) \end{aligned}$$ *where* $$NearPixFun\ (arg1\,, arg2) = \left(\left(floor\left(\frac{arg1}{10}\right) \times 10\right) + arg2\right) \quad (2)$$
	Step 5	***Repeat*** *the step 4 for* g_{i+1} *pixel and compute its nearest values* S_0g_{i+1H}, S_0g_{i+1M}, S_0g_{i+1L}, S_1g_{i+1H}, S_1g_{i+1M} *and* S_1g_{i+1L}.
	Step 6	***Choose*** *the best (minimum difference) stego-pixels* (g'_i, g'_{i+1}), *for* g'_i *value with* S_0g_{iH}, S_0g_{iM}, S_0g_{iL}, S_1g_{iH}, S_1g_{iM} *and* S_1g_{iL} *using Equation (3).* $$g'_i = argmin_{\{x\ in\ CPVj\}}\{|x - g_i|\} \quad (3)$$ *where* CPV_j *is the set* $[S_0g_{iH}, S_0g_{iM}, S_0g_{iL}, S_1g_{iH}, S_1g_{iM}, S_1g_{iL}]$ *of closest pixels with j number of possible values.* ***Repeat*** *this step for* g'_{i+1} *value with* S_0g_{i+1H}, S_0g_{i+1M}, S_0g_{i+1L}, S_1g_{i+1H}, S_1g_{i+1M} *and* S_1g_{i+1L}.
	Step 7	***If*** *the* g'_i *and* g'_{i+1} *pixel values* $\in$ *[0, 255] and the new difference* $d'_i = \left|g'_i - g'_{i+1}\right|$ *belongs to region-1 level (of Table 1) return/stop otherwise go to step 4.*
End		

Scheme 1. *Cont.*

Proposed RMDR embedding example is as follows.

Let		$g_i = 74$ *and* $g_{i+1} = 99$ *are the ith block pixels values of C, the secret message bits* $M = (10101101010 \ldots)_2$
Begin:		
	Step 1	***Read*** $n = 6 = (1\ 0\ 1\ 0\ 1\ 1)_2$ *bits from M,* ***generated*** *decimals are* $b_i = (1\ 0\ 1)_2 = (5)_{10}$ *and* $b_{i+1} = (0\ 1\ 1)_2 = (3)_{10}$.
	Step 2	***Found*** *respective* $SRD_{0(5)} = 5$, $SRD_{1(5)} = -1$ *against* $b_i = 5$ *and* $SRD_{0(3)} = 3$, $SRD_{1(3)} = 8$ *against* $b_{i+1} = 3$ *from Table 2.*
	Step-3	***Discarded*** *the* $SRD_{1(5)} = -1$, *because pixel right digit should be* $\in [0, 9]$.
	Step 4	***Generated*** *nearest pixels for* $g_i = 74$ *as* $S_0g_{iH} = 85$, $S_0g_{iM} = 75$ *and* $S_0g_{iL} = 65$ with $SRD_{0(5)} = 5$ *and* $\in [0, 255]$. $$S_0g_{iL} = 65 = NearPixFun\ ((74-10),\ 5)$$ $$S_0g_{iM} = 75 = NearPixFun\ (74,\ 5)$$ $$S_0g_{iH} = 85 = NearPixFun\ ((74+10),\ 5)$$
	Step 5	***Repeated*** *step 4 for* $g_{i+1} = 99$ *pixel and its nearest values with* $SRD_{0(3)} = 3$ *are* $S_0g_{i+1H} = 103$, $S_0g_{i+1M} = 93$ *and* $S_0g_{i+1L} = 83$. *On the other hand, the nearest values for* $g_{i+1} = 99$ *with* $SRD_{1(3)} = 8$ *are* $S_1g_{i+1H} = 108$, $S_1g_{i+1M} = 98$ *and* $S_1g_{i+1L} = 88$. $$S_0g_{i+1L} = 83 = NearPixFun\ ((99-10),\ 3) \qquad S_1g_{i+1L} = 88 = NearPixFun\ ((99-10),\ 8)$$ $$S_0g_{i+1M} = 93 = NearPixFun\ (99,\ 3) \qquad S_1g_{i+1M} = 98 = NearPixFun\ (99,\ 8)$$ $$S_0g_{i+1H} = 103 = NearPixFun\ ((99+10),\ 3) \qquad S_1g_{i+1H} = 108 = NearPixFun\ ((99+10),\ 8)$$
	Step 6	***Selected*** *the best closest* $g'_i = 75$ *and* $g'_{i+1} = 98$ *values from* $g'_i = 75 = argmin_{[85,75,65]}\{|74 - [85, 75, 65]|\}$, $g'_{i+1} = 98 = argmin_{[83,88,93,98,103,108]}\{|99 - [83, 88, 93, 98, 103, 108]|\}$
	Step 7	***Both*** $g'_i = 75$ *and* $g'_{i+1} = 98$ *pixel values* $\in [0, 255]$ *and the new difference* $23 = |75 - 98|$ *exists in region-1 level (of Table 1).*
End		

Scheme 1. Proposed RMDR embedding steps.

The above RMDR embedding method provides the embedding capacity of 3 bits per pixel (bpp), and its closest stego-pixel selection process provides good visual quality around the +38 dB peak signal-to-noise ratio (PSNR) of a stego-image. Furthermore, RMDR has the advantage of resisting RS-steganalysis detection attacks due to its digit replacement characteristics, as shown in Section 3.4.

2.2. Hybrid Embedding Method

The proposed hybrid embedding method concurrently utilized the digits and bits characteristics of pixels values to hide the secret data that confuse the statistical structural steganalysis methods. The proposed hybrid method partitioned the cover-image into two non-overlapping consecutive (horizontal) pixel blocks *i.e.*, $block = (g_1,\ g_2)$. The pixel difference $d = abs(g_1 - g_2)$ of each block is used to determine the region level of the block, as shown in Table 1. Furthermore, the pixel difference blocks belonging to region-1 and region-2 are employed by the RMDR (Section 2.1) and k-bit ALSB [9] embedding methods, respectively. However, from the experimental results, we found that some stego-blocks of region-2 can be switched to region-1 during the ALSB [9] embedding process. Therefore, the proposed method failed to recover 100% of the secret bits through the extraction process. For example, $(g_0,\ g_1)$ = (146, 178) and secret bits are (1010 0010), where its difference $d = |32|$, belongs to region-2 of Table 1. Therefore, the ALSB embedding and extraction process would be applied to hide and recover the secret bits. So, after applying ALSB embedding, the stego-block values are $(g'_0\ ,\ g'_1\ )$ = (154, 178), and its new difference $d' = |24|$, where this stego-block loses its region consistency from region-2 to region-1 of Table 1. Therefore, the ALSB-based block of region-2 would be considered as the RMDR region-1 based block during the extraction process and the secret data would not be recovered with 100% accuracy. Hence, a readjustment process as in Equation (4) is applied on the ALSB-based stego-block $(g'_0\ ,\ g'_1\ )$ when a region inconsistency problem occurs. This readjustment process computes the new stego-block $(g'_0\ ,\ g'_1\ )$ while maintaining the region's consistency and secret data. After applying Equation (4), the new $d' = |40|$ of the resultant stego-block $(g'_0,\ g'_1)$ = (138, 178) belongs to region-2 of Table 1, and 100% of the secret data can be recovered during the extraction process. Furthermore, the complete embedding steps are illustrated in Scheme 2.

$$(g'_0\ ,\ g'_1) = \begin{cases} (x'_0\ ,\ x'_1)\ \ if\ g'_0 \geqslant g'_1 \\ (x''_0\ ,\ x''_1)\ \ otherwise \end{cases} \tag{4}$$

where $(x'_0\ ,\ x'_1)$ and $(x''_0\ ,\ x''_1)$ pixels are computed as

$$(x'_0\ ,\ x'_1) = \begin{cases} \left(g'_0 + 2^k\ ,\ g'_1\right) & if\ \left|\left(g'_0 + 2^k\right) - g'_1\right| \in region2 \\ \left(g'_0 + 2^k,\ g'_1 - 2^k\right) & if\ \left|\left(g'_0 + 2^k\right) - \left(g'_1 - 2^k\right)\right| \in region2 \end{cases}$$

$$(x''_0\ ,\ x''_1\ ) = \begin{cases} \left(g'_0 - 2^k\ ,\ g'_1\right) & if\ \left|\left(g'_0 - 2^k\right) - g'_1\right| \in region2 \\ \left(g'_0 - 2^k,\ g'_1 + 2^k\right) & if\ \left|\left(g'_0 - 2^k\right) - \left(g'_1 + 2^k\right)\right| \in region2 \end{cases}$$

2.3. RMDR Extracting Method

The RMDR extracting method required the two stego-pixels as g'_i and g'_{i+1} of block(i) from stego-image (S) and Table 3 for extraction of stegoRDs. This extraction method extracts the RDs (*i.e.*, $ExRD_i$ and $ExRD_{i+1}$) of g'_i and g'_{i+1} and finds its equivalent b_i and b_{i+1} values from Table 3. Furthermore, the transformation and concatenation processes are applied on the extracted RDs. The RDMR extraction steps and its examples are given in Scheme 3.

Let	g_i *and* g_{i+1} *are the* ***i****th block pixels values of cover-image* ***C****,* ***M*** *be the secret message bits streams,* ***k*** *indicates the number of least bits for LSB embedding, Table 1 is used to identify the level of region-1 and region-2 difference range of pixel blocks.*	
Begin:		
	Step 1	***Partitioned*** *the C into two consecutive pixels with i no. of blocks in raster scan order,* $block_i = (g_i, g_{i+1})$.
	Step 2	***Calculate*** *the difference* $d_i = (g_{i+1} - g_i)$.
	Step 3	***If*** *the* $\lvert d_i \rvert$ *belongs to region-1 level of Table 1, apply RMDR embedding method (Section 2.1) with M to satisfy the following condition.* - *Stego-pixels values* g'_i *and* $g'_{i+1} \in [0, 255]$. - *The new difference* $d\prime_i \in$ *region-1 level of Table 1.*
	Step 4	***If*** *the* $\lvert d_i \rvert$ *belongs to region-2 level of Table 1, apply the k-bit ALSB OPAP with region-2 k secret bits (M) embedding method to satisfy the following condition.* - ***If*** *new difference* $\lvert d\prime_i \rvert \in$ *region-1 level of Table 1.* *Then the readjustment process is applied on* g'_i *and* g'_{i+1} *using Equation (4).*
	Step 5	***Repeat*** *Steps 1–5 until all M are embedded; if all cover blocks are traversed while M has not been embedded completely, restart Step 1 with new C.*
End		

Scheme 2. Proposed hybrid embedding steps.

Table 3. RMDR extraction table for StegoRDs.

ExRD	*b*
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	3
9	4

Let	*Stego-pixel* g'_i *and* g'_{i+1} *are the* ***i****th block pixels values of S. Table 3 , ExRD is consider as* $ExRD_i$ *and* $ExRD_{i+1}$ *and b is treated as* b_i *and* b_{i+1}.	
Begin:		
	Step 1	***Read*** g'_i *and* g'_{i+1} *pixels of ith block of S.*
	Step 2	***Extract*** *the RDs as* $ExRD_i$ *and* $ExRD_{i+1}$ *from* g'_i *and* g'_{i+1}*, respectively, i.e.,* $ExRD_i$ = *Mod* (g'_i, 10).
	Step 3	***Find*** *the* b_i *and* b_{i+1} *equivalent values against* $ExRD_i$ *and* $ExRD_{i+1}$ *from Table 3.*
	Step 4	***Convert*** *the decimal values of* b_i *and* b_{i+1} *into binary and concatenate the n = 6 (*n_5, n_4, n_3, n_2, n_1, n_0*) bits as a recovered M bit stream.*
End		

Proposed RMDR extraction example is as follows.

Let	*Stego-pixel* g'_i, g'_{i+1} = (75, 98) *are the ith block pixel values of S.*	
Begin:		
	Step 1	***Read*** g'_i = 75 *and* g'_{i+1} = 98 *pixels.*
	Step 2	***Extracted*** *RD's are* $ExRD_i$ = 5 *and* $ExRD_{i+1}$ = 8. *e.g.,* 5 = *Mod* (75, 10).
	Step 3	***Found*** *equivalent of* $ExRD_i$ = 5 *and* $ExRD_{i+1}$ = 8 *are* b_i = 5 *and* b_{i+1} = 3 *from Table 3.*
	Step 4	***Converted*** *binary and concatenated as* $b_i = (5)_{10} = (101)_2$ *and* $b_{i+1} = (3)_{10} = (011)_2$ *and* $(101011)_2$ *bits as a recovered six-bit stream.*
End		

Scheme 3. Proposed RMDR extraction steps.

Let	g'_i *and* g'_{i+1} *are the* ***i****th block pixels values of stego-image S.*	
Begin:		
	Step 1	***Partitioned*** *S into two consecutive pixels with i no. of blocks in raster scan order,* $block_i = \left(g'_i, g'_{i+1} \right)$.
	Step 2	***Compute*** *the difference* $d_{ri} = \left(g'_{i+1} - g'_i \right)$.
	Step 3	***If*** *the* $\lvert d_{ri} \rvert$ *belongs to region-1 level of Table 1, apply RMDR extraction method (Section 2.3); otherwise apply ALSB extraction using Table 1 with k-bit secret bits process.*
	Step 4	***Repeat*** *Steps 1–4 until all M is extracted from S.*
End		

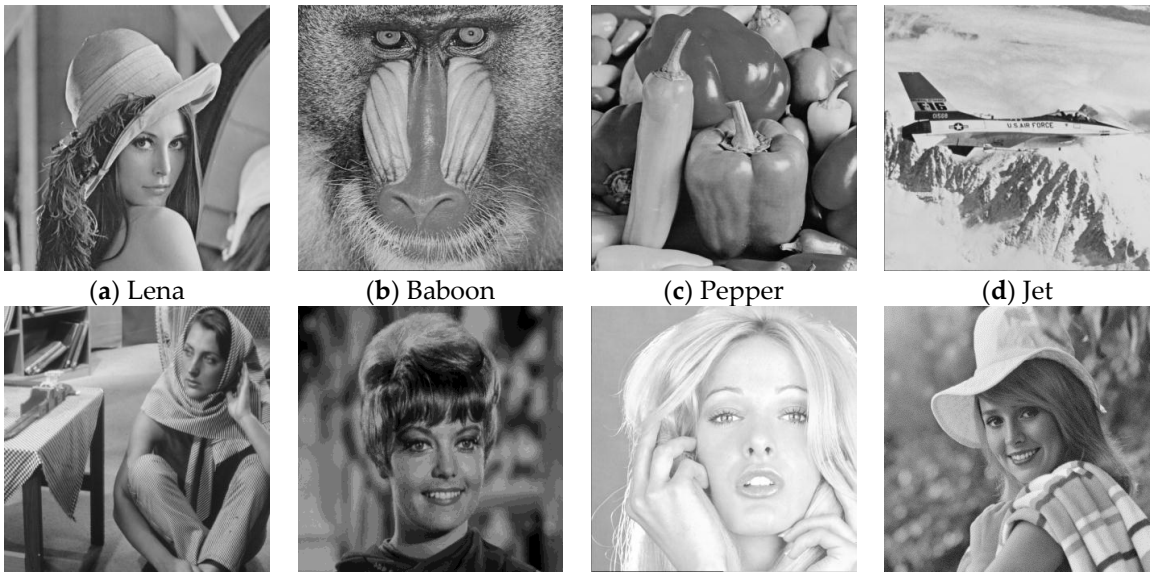
Scheme 4. Proposed hybrid extraction steps.

2.4. Hybrid Extraction Method

The hybrid extraction process required the stego-image as input and range table division as listed in Table 1. Similar to the embedding process, the stego-image S is partitioned into two consecutive non-overlapped pixel blocks, *i.e.*, $block = (g_1, g_2)$. If the difference of each block value $d = abs(g_1 - g_2)$ exists in the region-1 level (Table 1), RMDR extraction (Section 2.3) is applied; otherwise, the k-bit ALSB OPAP [9] extraction method is employed. The extraction steps are given in Scheme 4.

3. Experimental Results and Discussion

In this experimental section, the proposed hybrid method was implemented in MATLAB and tested on two well-known and standard image datasets. First, the proposed method was tested with the uncompressed color image database (UCID) [39], which consists of 1338 images with resolutions of 512 × 384 and 384 × 512. Furthermore, these RGB color images are converted into gray scale before testing. Second, we utilized the USC-SIPI [40] standard eight-bit (512 × 512, 256 × 256, and 1024 × 1024) test images, *i.e.*, Lena, Baboon, Pepper, Jet, Barbara, Zelda, Tiffany, and Elaine, as shown in Figure 2. The secret data were generated by a pseudo-random numbers generator. In the experiments, the same experimental procedure (fixed k = 4) is applied to our proposed method and other hybrid methods [19,25,27,28,34]. The performance comparisons are evaluated based on measuring the embedding capacity, PSNR, bpp, universal quality index (Q), and security by RS-analysis, pixel difference histogram analysis, and SPAM features under ensemble classifier steganalysis. Furthermore, these experimental results are analyzed and shown in Sections 3.1–3.6.



(**a**) Lena (**b**) Baboon (**c**) Pepper (**d**) Jet

(**e**) Barbara (**f**) Zelda (**g**) Tiffany (**h**) Elaine

Figure 2. Images for experiments (**a**–**h**).

3.1. Embedding Capacity and Visual Quality Analysis

This section analyzes the performance of hidden capacity and visual quality of proposed and existing methods in three parts. First, we compared the proposed hybrid method with existing well-known steganographic methods (*i.e.*, LSB, PVD [19,41]), as shown in Table 4. Secondly, the proposed method was compared with existing LSB-based hybrid methods (*i.e.*, Wu *et al.* [27], Yang *et al.* [34], Jung *et al.* [29], Khodaei *et al.* [28] and Wu *et al.* [25]) in Table 5. Third, the performance of the proposed method and existing hybrid methods are measured with complete UCID [39] and USC-SIPI [40] image datasets, as shown in Table 6.

The number of secret bits embedded into a stego-image is considered to be the embedding capacity. The highest value of embedding capacity indicates a good payload. For evaluating the visual imperceptibility of stego-images, PSNR and mean square error (MSE) were calculated as in Equation (5). H and W represent the height and width of the cover-image and g_i, g'_i represent cover and stego-pixels, respectively. The highest value of PSNR indicates the good visual quality of a stego-image with respect to its cover-image.

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad (5)$$

where $MSE = \frac{1}{H \times W}\sum_{i=1}^{H \times W}\left(g_i - g'_i\right)^2$.

The embedding capacity and PSNR performance statistics of proposed and singular steganographic methods are shown in Table 4 for eight stego-images. The results show that the average hidden capacity (800,109 bits) of the proposed method is higher than for 3-bit LSB, (Wu and Tsai [19]) PVD, and (Yang *et al.*'s [41]) adaptive LSB methods. The proposed method's PSNR was slightly lower than that of Wu and Tsai's method [19] but the hidden capacity of the proposed method is almost double that of Wu and Tsai's [19] (see Table 4). Moreover, Wu and Tsai's method [19] suffers from pixel histogram steganalysis [27].

Table 4. Performance comparison between the proposed hybrid embedding method and singular steganographic methods.

Parameters	Methods	Lena	Baboon	Pepper	Jet	Barbara	Zelda	Tiffany	Elaine	Average
PSNR (dB)	Proposed	39.19	38.03	39.34	39.18	37.92	39.56	39.24	39.50	39.00
	3-bit LSB	37.90	37.90	37.91	37.95	37.92	37.92	37.89	37.92	37.91
	Wu and Tsai [19]	41.10	36.98	41.55	40.42	36.33	42.94	41.48	41.88	40.34
	Yang *et al.* [41]	39.31	39.16	39.06	39.55	39.16	39.00	39.12	39.01	39.17
Capacity (bits)	Proposed	793,810	820,776	792,384	795,728	824,084	788,516	792,864	791,994	800,019
	3-bit LSB	786,432	786,432	786,432	786,432	786,432	786,432	786,432	786,432	786,432
	Wu and Tsai [19]	409,776	456,952	405,424	409,531	450,650	339,918	398,980	408,582	417,447
	Yang *et al.* [41]	757,332	785,572	786,014	735,236	786,012	778,014	777,888	760,016	770,761

Table 5. Performance comparison of existing hybrid LSB-based (PVD, EMD, and MPE) methods against the proposed method.

Parameters	Methods	Lena	Baboon	Pepper	Jet	Barbara	Zelda	Tiffany	Elaine	Average
PSNR (dB)	Proposed	39.19	38.03	39.34	39.18	37.92	39.56	39.24	39.50	39.00
	Wu *et al.* [27]	37.12	35.30	37.20	36.98	34.79	37.63	37.25	37.28	36.70
	Jung *et al.* [29]	36.28	35.94	36.10	36.20	36.02	36.05	35.12	35.92	35.95
	Yang *et al.* [34]	38.71	36.19	38.92	38.56	35.57	39.78	39.11	39.26	38.26
	Khodaei *et al.* [28]	37.56	34.85	35.88	36.29	32.91	38.49	37.78	38.17	36.49
	Wu *et al.* [25]	35.10	35.10	35.10	35.10	35.10	35.10	35.10	35.10	35.10
Capacity (bits)	Proposed	793,810	820,776	792,384	795,728	824,084	788,516	792,864	791,994	800,019
	Wu *et al.* [27]	765,969	717,749	768,455	770,176	740,147	776,196	766,663	760,170	758,191
	Jung *et al.* [29]	786,432	786,441	786,586	786,475	786,406	786,647	786,559	786,440	786,498
	Yang *et al.* [34]	765,969	717,749	768,455	770,176	740,147	776,196	766,663	760,170	758,191
	Khodaei *et al.* [28]	791,443	809,435	790,299	792,443	811,747	787,887	790,503	788,356	795,264
	Wu *et al.* [25]	639,761	603,894	620,920	650,362	626,994	641,866	643,305	615,116	630,227

From the experimental results, as shown in Table 5, the proposed method has the highest average hidden capacity and simultaneously has higher PSNR as compared with existing LSB-based hybrid methods. This is due to the combination of RMDR and adaptive LSB methods because RMDR produces the good visual quality of stego-image at 3 bpp while the adaptive LSB method ensures the highest payload up to 800,019 bits. Finally, the performance of payload and PSNR are compared for UCID [39] and USC-SIPI [40] image datasets, as shown in Table 6. The experimental results show that the proposed method's average payload in UCID [39] (554,156 bits) and the USC-SIPI [40] (1,636,102 bits) database are higher than for the existing methods. Similarly, the proposed method, PSNR, in UCID [39]

(38.88 dB) and USC-SIPI [40] (38.32 dB) are the highest among others. This indicates that the proposed method outperformed the existing hybrid embedding method in simultaneously achieving high payload and visual quality. This is due to the fact that the proposed method keeps both RMDR (good visual quality) and adaptive LSB (high payload) advantages intact to efficiently utilize lower and higher texture areas during embedding procedure.

Table 6. Performance comparison with UCID [39] and USC-SIPI [40] image datasets of proposed and existing hybrid methods.

Methods	Average Capacity		Average PSNR		Average Q	
	UCID [39]	USC-SIPI [40]	UCID [39]	USC-SIPI [40]	UCID [39]	USC-SIPI [40]
Proposed	554,156	1,636,102	38.88	38.32	0.9988	0.9952
Wu *et al.* [27]	514,375	150,3772	36.67	35.99	0.9979	0.9919
Yang *et al.* [34]	514,375	150,3772	37.91	37.19	0.9984	0.9940
Jung *et al.* [29]	540,682	1,591,207	34.48	34.12	0.9951	0.9862
Khodaei *et al.* [28]	549,448	1,623,681	35.02	34.72	0.9955	0.9873
Wu *et al.* [25]	481,140	141,6278	35.10	35.10	0.9972	0.9890

Furthermore, Figure 3 illustrates the bit plane decomposition of cover and proposed stego-images. The bit plane results show that the stego-image is almost visually identical to its cover-image, and can resist the bit plane analysis. Similarly, in Figure 4, the visual distortion artifacts of proposed and recent hybrid methods are compared for the Lena image. It shows that the proposed method has less human perceivable differences than compared methods. This is due to the fact that the proposed method uses the RMDR closest pixels selection process, which computes the best stego-pixels against its cover pixels.

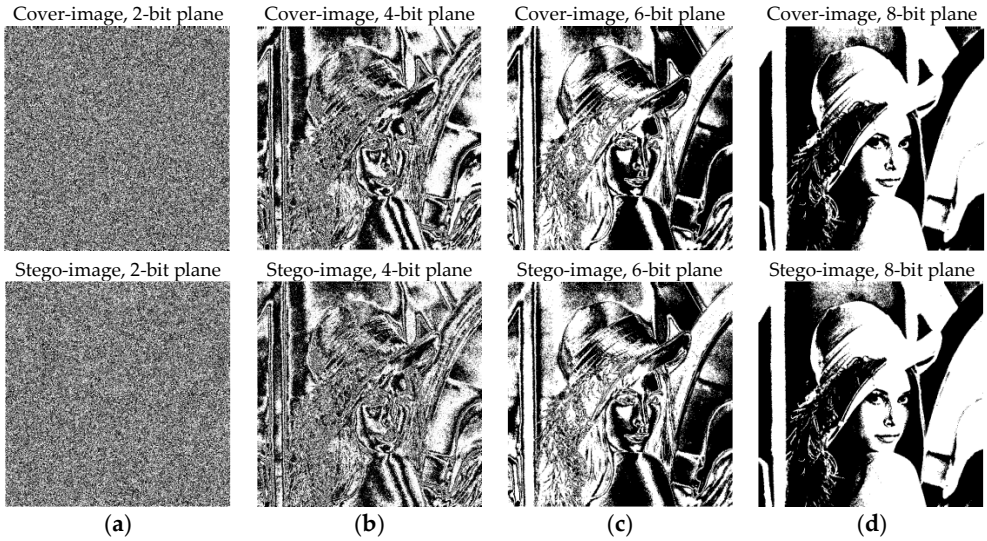


Figure 3. Bit plane comparison of cover and stego-images (**a**–**d**).

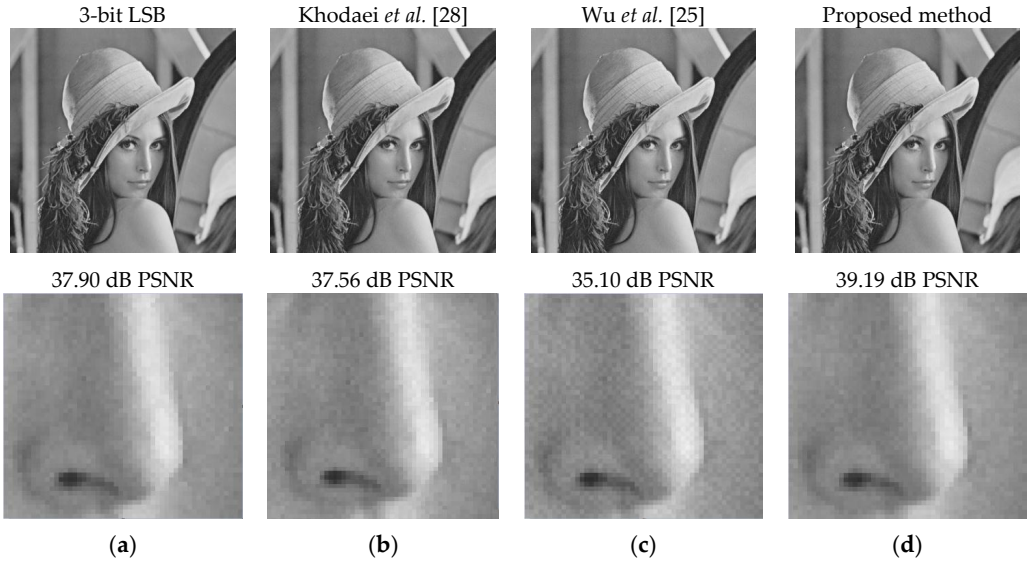


Figure 4. Stego-images and its specific zoomed area of (**a**) 3-bit LSB; (**b**) Khodaei *et al.* [28]; (**c**) Wu *et al.* [25]; and (**d**) the proposed method.

3.2. Universal Quality Index Analysis

A universal quality index Q measures the visual quality of an image [42]. Let $Y_j = \{ Y_j \mid j = 1,2,3,\ldots,N\}$ and $Z_j = \{ Z_j \mid j = 1,2,3,\ldots,N\}$ be the cover-image and stego-image, respectively. The quality Q is computed as in Equation (6):

$$Q = \frac{4 \times \left(\acute{O}_{YZ}\right) \times Y'' \times Z''}{\left(\left(\acute{O}_Y\right)^2 + \left(\acute{O}_Z\right)^2\right)\left[(Y'')^2 + (Z'')^2\right]} \tag{6}$$

where

$$Y'' = \frac{1}{N}\sum_{j=1}^{N} Y_j, \quad Z'' = \frac{1}{N}\sum_{j=1}^{N} Z_j$$

$$\left(\acute{O}_Y\right)^2 = \frac{1}{N-1}\sum_{j=1}^{N}\left(Y_j - Y''\right)^2, \quad \left(\acute{O}_Z\right)^2 = \frac{1}{N-1}\sum_{j=1}^{N}\left(Z_j - Z''\right)^2$$

$$\acute{O}_{YZ} = \frac{1}{N-1}\sum_{j=1}^{N}\left(Y_j - Y''\right) \times \left(Z_j - Z''\right)$$

The range of Q is $[-1, +1]$. The value 1 represents the best quality when $Y = Z$, or the stego-image is identical to its cover-image. From Table 7, the proposed method shows the value of Q against existing (3-LSB, Yang *et al.* [34], Khodaei *et al.* [28], and Wu *et al.* [25]) methods. Moreover, the value Q of the proposed method is closer to 1. This shows that the proposed method has similar fidelity between the cover and stego-image against the compared methods.

Table 7. Universal quality index (Q) of proposed and existing LSB-based methods by Wang and Bovik [42].

Methods	Lena	Baboon	Pepper	Jet	Barbara	Zelda	Tiffany	Elaine	Average
Proposed	0.9983	0.9979	0.9987	0.9982	0.9972	0.9988	0.9985	0.9983	0.9982
3-bit LSB	0.9977	0.9971	0.9982	0.9976	0.9983	0.9968	0.9939	0.9975	0.9971
Yang *et al.* [34]	0.9981	0.9955	0.9985	0.9979	0.9969	0.9979	0.9952	0.9980	0.9973
Khodaei *et al.* [28]	0.9975	0.9940	0.9971	0.9965	0.9944	0.9972	0.9937	0.9977	0.9960
Wu *et al.* [25]	0.9959	0.9948	0.9967	0.9957	0.9968	0.9943	0.9893	0.9956	0.9949

3.3. Embedding Capacity versus PSNR

The embedding capacity *vs.* the PSNR for the proposed and existing methods [25,27,28,34] are depicted in Figure 5a–d except for the similar results for the first four test images. In Figure 5a, the methods were tested on the Lena image. The respective PSNR values at 20,000 hidden bits are 53.78 dB, 55.96 dB, 63.98 dB, 54.80 dB, and 55.70 dB for Wu *et al.*, Yang *et al.*, Wu *et al.*, Khodaei *et al.*, and the proposed methods. The proposed method reached its maximum of 793,810 hidden bits when the PSNR was 39.19 dB while the other three methods reached their maximum of 791,443 bits with PSNR at 37.56 dB. The experiment on the Baboon image showed that the maximum hidden capacity and PSNR of Wu *et al.* [27] (717,749 bits, 35.30 dB), Yang *et al.* [34] (717,749 bits, 36.19 dB), Wu *et al.* [25] (603,894 bits, 35.10 dB), Khodaei *et al.* [28] (809,435 bits, 34.85 dB), and the proposed method had a maximum of 820,776 bits with 38.03 dB PSNR, as depicted in Figure 5b. The proposed method gained up to +103,525 hidden bits and +1.86 PSNR against Yang *et al.* [34]. For the Pepper image, the embedding capacity of the proposed method had a maximum of 792,384 bits at 39.34 dB PSNR, as shown in Figure 5c. The PSNR in the Jet image at 20,000 embedding bits recorded for Wu *et al.* [27] is 53.67 dB, for Yang *et al.* [34] is 55.83 dB, for Wu *et al.* [25] is 64.00 dB, for Khodaei *et al.* [28] is 53.80 dB, and for the proposed method is 55.62 dB. The proposed method had a maximum embedding capacity and PSNR around 795,728 bits with 39.18 dB PSNR.

Therefore, the graphs analysis in Figure 5 illustrates that the proposed method can achieve good and almost higher PSNR values without considering the different levels of embedding payload. It shows that the proposed method produces good visual symmetry irrespective of embedding payload. Among these test images, a prominent gain was achieved for the Baboon image. This shows that the proposed method is also suitable for both types of texture-based images and works better with higher texture images e.g., Baboon.

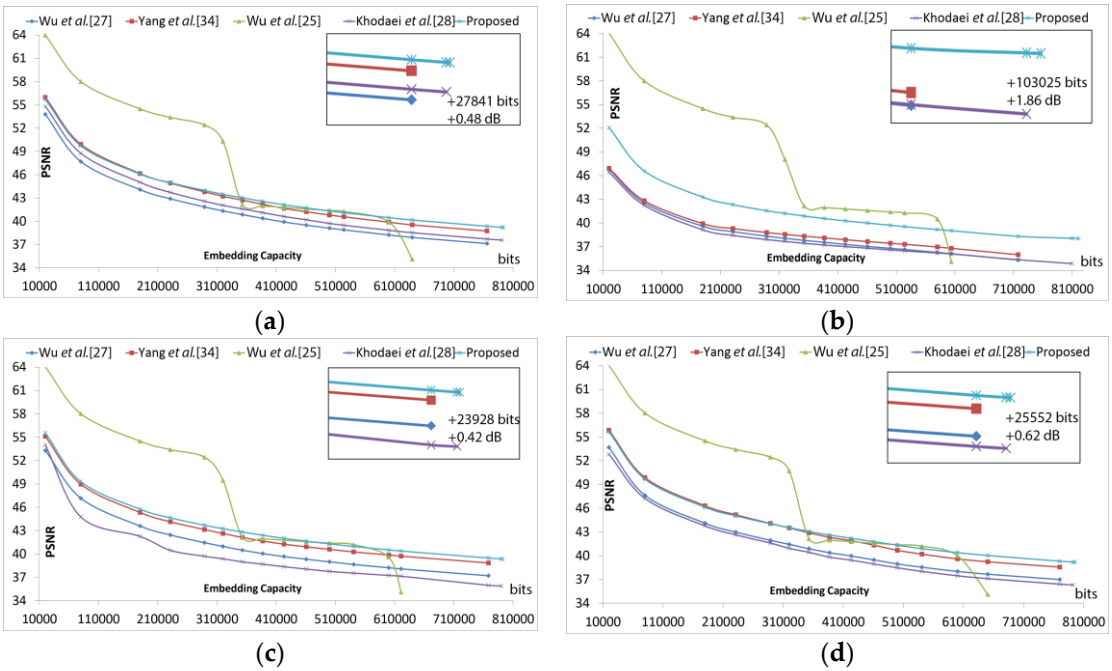


Figure 5. Comparison graphs for various embedding capacities *vs.* PSNR: (**a**) Lena; (**b**) Baboon; (**c**) Pepper; (**d**) Jet.

3.4. Security against Statistical RS-Steganalysis

The security of the proposed method against statistical RS-steganalysis [10] plays a significant role in detecting the hidden data inside the stego-images. In this section, the process of evaluating security

against RS-analysis is divided into two parts. Firstly, RS-analysis is compared with the proposed RMDR and 3-bit LSB embedding approaches (see Figure 6). Secondly, RS-analysis is evaluated for the proposed hybrid approach (see Figure 7).

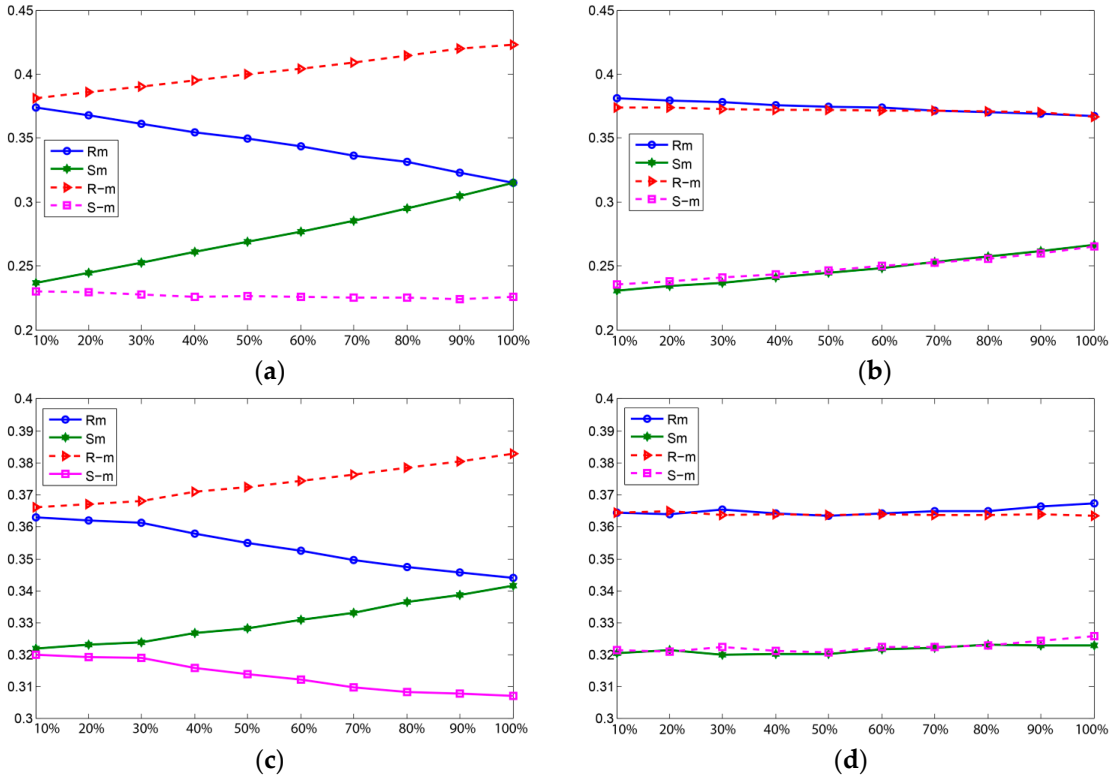


Figure 6. RS-analysis graphs for 3-bit LSB *vs.* RMDR of stego-images. (**a**) Lena 3-bit LSB; (**b**) Lena RMDR; (**c**) Baboon 3-bit LSB; (**d**) Baboon RMDR.

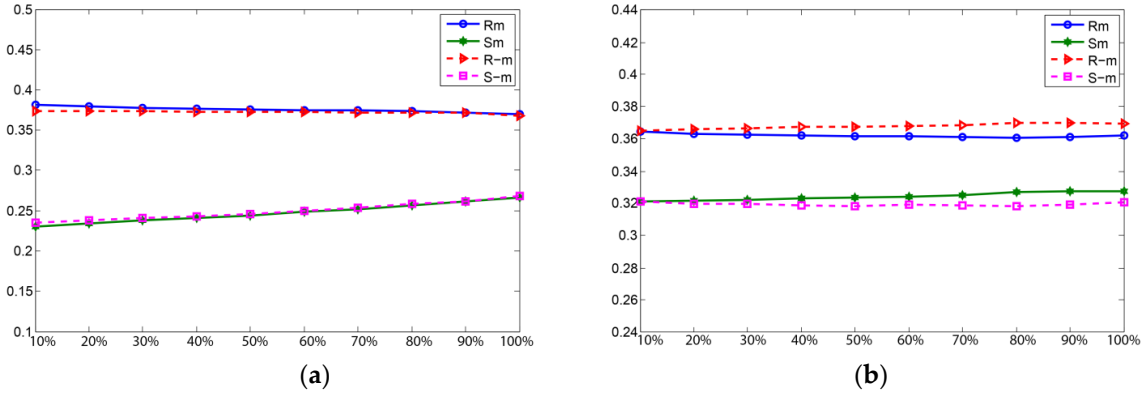


Figure 7. RS-analysis graphs of Lena (**a**) and Baboon (**b**) images by the proposed method.

The RS-steganalysis method presents a discrimination function (DF) with flipping masks as M and –M, where M and –M are $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$, respectively. R_{M}, S_{M}, $R_{-\mathrm{M}}$, and $S_{-\mathrm{M}}$ indicate the proportion of blocks, where the magnitude of DF increases or decreases on applying each block. If the parameters satisfies $R_{\mathrm{M}} \approx R_{-\mathrm{M}} > S_{\mathrm{M}} \approx S_{-\mathrm{M}}$, it indicates that there is no hidden data in the respective image. When an image has hidden data, $R_{-\mathrm{M}}$ and S_{M} increases, whereas R_{M} and $S_{-\mathrm{M}}$ decreases and exposed by RS-analysis.

The RS detection results can be seen in Figure 6a–d with 3-bit LSB and RMDR methods for the first two images, Lena and Baboon. In Figure 6a–d, the x-axis indicates the percentage of secret data inside the stego-image and the y-axis denotes the relative percentages of regular (R_M, R_{-M}) and singular (S_M, S_{-M}) groups when applying the above masks (M, $-$M). The comparison of RS-analysis between the RMDR and 3-bit LSB embedding methods is due to the similar embedding capacity of 3 bpp. The 3-bit LSB difference between the singular and regular groups increases with the addition of embedding capacity, as shown in Figure 6a,c. In the RMDR method, Figure 6b,d retained the closest differences in singular and regular groups up to 100% embedding capacity and proved the undetectability against RS-steganalysis of the RMDR method.

Figure 7a,b shows the RS detection analysis of the Lena and Baboon images with the proposed hybrid approach. In RS-analysis graphs, stego-images had both singular and regular parameters close to each other even with an increase in hidden data bits. This indicates that the proposed method has high security against statistical RS-analysis.

3.5. Pixel Difference Histogram Analysis

A pixel difference histogram is one of the potential steganalysis methods to expose the secret data of stego-images. The pixel difference histogram is computed by taking the differences of neighboring pixels with fall-off ranges between cover and stego-image. Figure 8 shows the pixel difference histograms of the Lena and Baboon stego-images using the Wu *et al.* method [25], the Khodaei *et al.* method [28], and the proposed method. In the case of Lena histogram (a), it is observed that the proposed stego-image histogram is well preserved against Wu *et al.* [25] and Khodaei *et al.* [28] methods. Similarly, for the Baboon stego-image comparison, Wu *et al.*'s method lost symmetry to keep its curves close to its cover-image difference histogram [25]. However, the proposed hybrid method provides more security by keeping the pixel difference histogram closer to the cover-image; it did not generate any noticeable artifacts under pixel difference histogram steganalysis detection attacks.

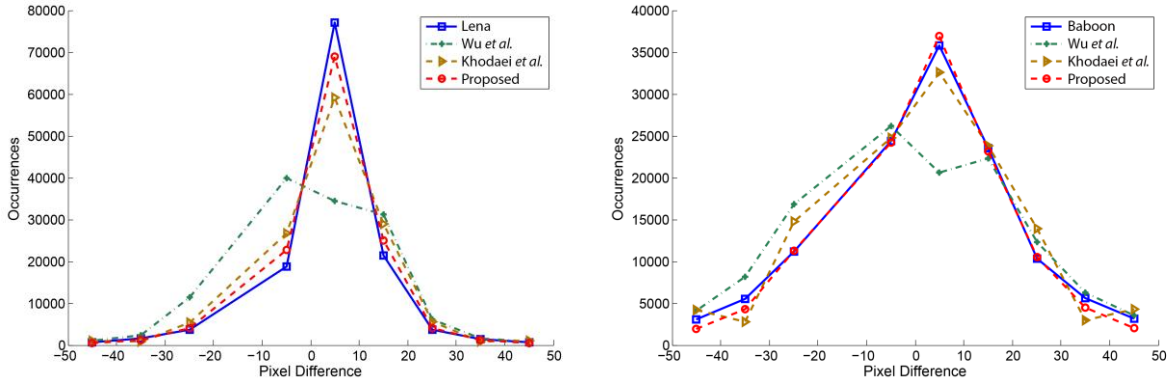


Figure 8. Pixel difference histograms of cover and stego-images of the proposed method compared to the methods of Wu *et al.* [25] and Khodaei *et al.* [28] (**a**,**b**).

3.6. Undetectability under SPAM Analysis Using Ensemble Classifier

In this section, we analyzed the proposed method using an ensemble classifier with state-of-the-art modern steganalysis SPAM-based features [43]. The second order SPAM 686 feature set steganalyzer is very effective at detecting stego-images. In our experiment, the ensemble classifier and SPAM features are obtained from [38]. These features are evaluated on both UCID [39] and USC-SIPI [40] image datasets, where 500 cover and 500 stego-images are used for training and the rest are used for testing. For an undetectability comparison, the proposed method and two state-of-the-art LSB matching methods known as ± 1 embedding and HUGO [14] are employed, as shown in Table 8. Table 8 consists

of columns, namely bit rate as bits per pixel (bpp), true positive, false positive, true negative, false negative, and finally the detection error rate of the steganalysis method. To evaluate the performance, the higher classification error rate indicates the higher undetectability of a steganography approach.

Table 8. Undetectabilityperformance under SPAM steganalysis with ensemble classifier for the proposed method as compared with the LSB matching and HUGO embedding methods.

Bit Rate (bpp)	Method	TP	FP	TN	FN	Error rate
0.2	Proposed	228	249	251	272	52.10%
	LSBM (±1)	421	174	326	79	25.30%
	HUGO	234	252	248	266	51.80%
0.4	Proposed	276	267	233	224	49.10%
	LSBM (±1)	443	102	398	57	15.90%
	HUGO	279	259	241	221	48.00%
0.6	Proposed	301	228	272	199	42.70%
	LSBM (±1)	453	55	445	47	10.20%
	HUGO	298	210	290	202	41.20%
0.8	Proposed	336	155	345	164	31.90%
	LSBM (±1)	478	38	462	22	06.00%
	HUGO	339	149	351	161	31.00%
1.0	Proposed	441	103	397	59	16.20%
	LSBM (±1)	497	14	486	3	01.70%
	HUGO	446	106	394	54	16.00%

As from Table 8, when the payload is 0.2 bpp, the proposed method has a higher error rate of 52.10%, while the LSBM (±1) and HUGO [14] had 25.30% and 51.80%, respectively. Generally, Table 8 shows that the proposed method has a higher detectability error rate than LSBM (±1) embedding method. Our method has a higher detectability error rate because the proposed method required fewer pixels to embed secret bits than the LSBM (±1) method. Suppose, in the worst case of LSBM (±1) embedding, it took (512 × 512) = (262,144) pixels to embed 262,144 secret bits. In the case of the proposed method, 85,948 pixels would be required to embed 262,144 bits due to the 3.05 bpp average embedding rate. So, the rest of the pixels in the proposed method would be unmodified, which would create less distortion from the artifacts' impact on the stego-image during feature extraction. In addition, the proposed method has a similar error rate to the HUGO [14] method, but a lower computational complexity [14]. The overall results indicate that the proposed method has high undetectability at a lower embedding rate. However, for a higher embedding rate, SPAM + ensemble classifier can successfully steganalyze all the embedding methods, *i.e.*, proposed, LSBM (±1), and HUGO [14].

4. Conclusions

In this work, we have presented a novel hybrid steganographic method with high payload and good visual symmetry, based on the adaptive LSB and RMDR methods. In order to conceal secret data, texture areas of the cover images are exploited according to the absolute difference of pixel pairs. Generally, lower texture areas of cover images are more noise sensitive to the higher texture areas. However, to embed secret data for low texture areas, we presented a closest stego-pixel selection process in the proposed RMDR method. Similarly, to obtain a larger payload in high texture areas, we employed the adaptive LSB embedding method to fully utilize the different variation of higher texture areas.

Compared with related LSB-based hybrid embedding approaches, the proposed method has significant advantages. First, the proposed method efficiently utilized the image texture areas against the PVD, ALSB, LSB + PVD, LSB + EMD + MPE methods, thereby enabling us to produce an embedded image with a significantly higher payload. Secondly, the proposed method reduces the visual distortion artifacts caused by different readjusting phases of the falling-off boundary, and underflow or overflow

problems, which are serious in other hybrid LSB + PVD methods. Finally, the proposed method is able to resist statistical RS detection attack and pixel difference histogram attack, and has undetectability for a lower rate of bits per pixels embedding against modern nonstructural steganalysis, *i.e.*, SPAM + ensemble classifier.

The proposed method, however, suffers from the following limitations. The nonstructural feature-based (SPAM + Ensemble classifier) steganalysis detection rate of our approach is essentially high at larger embedding bits per pixels. Second, the texture estimation is limited to two pixel pairs because it only considers a single (horizontal) direction. Third, there is no measure taken to encrypt secret data before the embedding process.

In the future, besides the merits achieved in this paper, we will attempt to improve in the following directions. Different pixel pair directions (*i.e.*, diagonally, vertically) should be investigated to find a more efficient texture estimation for the embedding process. Secondly, a statistical model should be investigated, before and after embedding secret data, to minimize the embedding distortion artifacts from modern steganalysis detection attacks. Third, state-of-the-art compression methods should be investigated and applied to minimize the size of secret data before embedding, to retain undetectability against modern steganalysis. Finally, encryption of secret data should be investigated to enhance the security of secret messages.

Acknowledgments: The work was supported by the National University of Science and Technology, Islamabad, Pakistan under faculty development program abroad (grant number 0972/F008/HRD/FDP-14/); the Ministry of Education, Malaysia under the University of Malaya (High Impact Research Grant UM.C/625/1/HIR/MoE/FCSIT/17); and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2015R1D1A1A01058019). We thank the anonymous reviewers for their valuable suggestions that improved the clarity of this article.

Author Contributions: All authors discussed the contents of the manuscript and contributed to its preparation. Mehdi Hussain and Ainuddin Wahid Abdul Wahab designed and implemented the proposed scheme; Noman Javed and Ki-Hyun Jung analyzed the simulation data and wrote the paper.

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

References

1. Fan, C.-I.; Tseng, Y.-F. Anonymous Multi-Receiver Identity-Based Authenticated Encryption with CCA Security. *Symmetry* **2015**, *7*, 1856–1881. [CrossRef]
2. Shahzad, A.; Lee, Y.-K.; Kim, S.; Xiong, N.; Choi, J.-Y.; Cho, Y. Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information. *Symmetry* **2015**, *7*, 1176–1210. [CrossRef]
3. Katzenbeisser, S.; Petitcolas, F. *Information Hiding Techniques for Steganography and Digital Watermarking*; Artech House: Boston, MA, USA, 2000.
4. Subhedar, M.S.; Mankar, V.H. Current status and key issues in image steganography: A survey. *Comput. Sci. Rev.* **2014**, *13*, 95–113. [CrossRef]
5. Kougianos, E.; Mohanty, S.P.; Mahapatra, R.N. Hardware assisted watermarking for multimedia. *Comput. Electr. Eng.* **2009**, *35*, 339–358. [CrossRef]
6. Kuo, W.-C.; Kuo, S.-H.; Wuu, L.-C. Multi-Bit Data Hiding Scheme for Compressing Secret Messages. *Appl. Sci.* **2015**, *5*, 1033–1049. [CrossRef]
7. Lee, C.F.; Weng, C.Y.; Sharma, A. Steganographic access control in data hiding using run-length encoding and modulo-operations. *Secur. Commun. Netw.* **2016**, *9*, 139–148. [CrossRef]
8. Collins, J.C.; Agaian, S.S. Taxonomy for spatial domain LSB steganography techniques. In *SPIE Sensing Technology+ Applications*; International Society for Optics and Photonics: Baltimore, MD, USA, 2014; Volume 9120, p. 912006.
9. Chan, C.-K.; Cheng, L.-M. Hiding data in images by simple LSB substitution. *Pattern Recognit.* **2004**, *37*, 469–474. [CrossRef]
10. Fridrich, J.; Goljan, M.; Du, R. Reliable detection of LSB steganography in color and grayscale images. In Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges, New York, NY, USA, 5 October 2001; pp. 27–30.

11. Fillatre, L. Adaptive steganalysis of least significant bit replacement in grayscale natural images. *IEEE Trans. Signal Process.* **2012**, *60*, 556–569. [CrossRef]
12. Zhang, J.; Cox, I.J.; Doërr, G. Steganalysis for LSB matching in images with high-frequency noise. In Proceedings of the IEEE 9th Workshop on Multimedia Signal Processing, Crete, Greece, 1–3 October 2007; pp. 385–388.
13. Al-Dmour, H.; Al-Ani, A. Quality optimized medical image information hiding algorithm that employs edge detection and data coding. *Comput. Methods Programs Biomed.* **2016**, *127*, 24–43. [CrossRef] [PubMed]
14. Pevný, T.; Filler, T.; Bas, P. Using high-dimensional image models to perform highly undetectable steganography. In *Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 161–177.
15. Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain, 2–5 December 2012; pp. 234–239.
16. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain. *EURASIP J. Inf. Secur.* **2014**, *2014*, 1–13. [CrossRef]
17. Li, B.; Wang, M.; Huang, J.; Li, X. A new cost function for spatial image steganography. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014; pp. 4206–4210.
18. Sedighi, V.; Fridrich, J.; Cogranne, R. Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model. In *IS&T/SPIE Electronic Imaging*; International Society for Optics and Photonics: San Francisco, CA, USA, 2015.
19. Wu, D.-C.; Tsai, W.-H. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.* **2003**, *24*, 1613–1626. [CrossRef]
20. Lee, Y.-P.; Lee, J.-C.; Chen, W.-K.; Chang, K.-C.; Su, J.; Chang, C.-P. High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Inf. Sci.* **2012**, *191*, 214–225. [CrossRef]
21. Balasubramanian, C.; Selvakumar, S.; Geetha, S. High payload image steganography with reduced distortion using octonary pixel pairing scheme. *Multimedia Tools Appli.* **2014**, *73*, 2223–2245. [CrossRef]
22. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
23. Wang, X.-T.; Chang, C.-C.; Lin, C.-C.; Li, M.-C. A novel multi-group exploiting modification direction method based on switch map. *Signal Process.* **2012**, *92*, 1525–1535. [CrossRef]
24. Kim, C. Data hiding by an improved exploiting modification direction. *Multimedia Tools Appl.* **2014**, *69*, 569–584. [CrossRef]
25. Wu, K.-S.; Liao, W.-D.; Lin, C.-N.; Chen, T.-S. A high payload hybrid data hiding scheme with LSB, EMD and MPE. *Imag. Sci. J.* **2014**, *63*, 174–181. [CrossRef]
26. 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]
27. Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEEE Proc. Vis. Image Signal Process.* **2005**, *152*, 611–615. [CrossRef]
28. Khodaei, M.; Faez, K. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image Process.* **2012**, *6*, 677–686. [CrossRef]
29. Jung, K.-H. High-capacity steganographic method based on pixel-value differencing and LSB replacement methods. *Imag. Sci. J.* **2010**, *58*, 213–221. [CrossRef]
30. Tsai, Y.-Y.; Chen, J.-T.; Chan, C.-S. Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding. *Int. J. Netw. Secur.* **2014**, *16*, 359–364.
31. Jung, K.-H.; Ha, K.-J.; Yoo, K.-Y. Image data hiding method based on multi-pixel differencing and LSB substitution methods. In Proceedings of the International Conference on Convergence and Hybrid Information Technology, Daejeon, South Korea, 28–30 August 2008.
32. Zaker, N.; Hamzeh, A. A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. *Multimedia Tools Appl.* **2012**, *58*, 147–166. [CrossRef]
33. Sajedi, H.; Jamzad, M. HYSA: hybrid steganographic approach using multiple steganography methods. *Secur. Comm. Netw.* **2011**, *4*, 1173–1184. [CrossRef]

34. Yang, C.-H.; Weng, C.-Y.; Wang, S.-J.; Sun, H.-M. Varied PVD + LSB evading detection programs to spatial domain in data embedding systems. *J. Syst. Softw.* **2010**, *83*, 1635–1643. [CrossRef]
35. Huang, H.-S. A combined image steganographic method using multi-way pixel-value differencing. In Proceedings of the Sixth International Conference on Graphic and Image Processing (ICGIP 2014), Beijing, China, 24–25 October 2015.
36. Shen, S.; Huang, L.; Tian, Q. A novel data hiding for color images based on pixel value difference and modulus function. *Multimedia Tools Appl.* **2015**, *74*, 707–728. [CrossRef]
37. Petitcolas, F.A.; Anderson, R.J. Evaluation of copyright marking systems. In Proceedings of the IEEE International Conference on Multimedia Computing and Systems, Florence, Italy, 7–11 June 1999.
38. Implementation of the Ensemble Classifier (Using Weka) and the SPAM Features + HUGO Algorithm. Available online: http://dde.binghamton.edu/download/ (accessed on 20 April 2016).
39. Schaefer, G.; Stich, M. UCID: An uncompressed color image database. In Proceedings of the SPIE, Storage and Retrieval Methods and Applications for Multimedia 2004, San Jose, CA, USA, 18 January 2004.
40. The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 1 September 2015).
41. Yang, H.; Sun, X.; Sun, G. A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering* **2009**, *18*, 509.
42. Wang, Z.; Bovik, A.C. A universal image quality index. *IEEE Signal Process. Lett.* **2002**, *9*, 81–84. [CrossRef]
43. Pevny, T.; Bas, P.; Fridrich, J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 215–224. [CrossRef]