Information EmbeddingAlgorithm based on Diamond Encoding Scheme withDifferent-base Digits

Samer Atawneh*
Saudi Electronic University
Riyadh 11673, Saudi Arabia
+966112613500
satawneh@seu.edu.sa

Hussein Al Bazar
Arab Open University
Saudi Arabia
+966138315415
Halbazar@arabou.edu.sa

Imran Usman
Saudi Electronic University
Riyadh, Saudi Arabia
+966112613500
i.usman@seu.edu.sa

Putra Sumari
UniversitiSainsMalaysia
(USM)Malaysia
+6046533615
putras@cs.usm.my

* Corresponding author: Tel: +966112613500. Ext. 1012

***Abstract*—This paper presents a new informationembedding algorithm based on the diamond encoding (DE)scheme with different base-digits. The DE scheme conveys a large payload while maintaining image quality. However, it does not support embedding of digits with different bases, which is vital for any embedding method that considers image quality. The proposed algorithm produces stego-images with lower distortion than DE by embedding different-base digits into the pixel pairs of the cover image. It divides secret information into two payloads in an optimal manner and embeds each payload into the cover image using a different base. Experimental results verify that the proposed algorithm is more efficient in embedding compared with other state-of-the-art techniques in terms of image quality and embedding payload. Theproposed algorithm is also attacked by well-known steganalysis software. Resultsshow that the proposed algorithm is robust against steganalysis attacks such as RS-steganalysis and PVD histogram analysis.**

Keywords-Image steganography; least significant bit (LSB); Pixel value differencing (PVD); diamond encoding (DE)

I. INTRODUCTION

Steganography is the art and science of incorporating secret information into other digital carriers (image, text, audio, video, etc.) to communicate such secret information[1; 2]. This technique is significant in today's digital world, in which large amounts of information are frequently and easily exchanged over the Internet by using email or other digital communication methods.A digital image is one of the most familiar multimedia file types readily available online. This availability is made possible by free Web-hosting sites (e.g., Instagram), and social networks (e.g., Facebook), wherecollections of images can be downloaded, uploaded, and viewed daily. Digital images are considered superior choices for hiding secret information because they are insensitive to human perception [3; 4].Imperceptibility and embedding payload are the most important properties that characterize the performance of any embedding method [5; 6; 7; 8]. Spatial-domain image steganography can embed large payload sizes [9], such as least significant bit (LSB) [10], palette-based [11], pixel value differencing (PVD) [12], and diamond encoding (DE) [13]. A recent classification of steganography methods is specified by [14].

LSB steganography embeds secret message bits in the LSBs of sequentially or randomly selected pixels of the cover image. The PVD steganography, proposed by Wu and Tsai [12], is another commonly used embedding scheme in digital images. In PVD, the difference value between two or more adjacent pixels is used to embed secret information. The difference value controls the embedding payload; that is, the higher the difference value, the greater the amount of secret information that can be embedded, consequently leading to high embedding payload. Wang et al. [15] developed the PVD concept to produce a new steganographic method based on the use of a modulus function (M-PVD). This method exploits PVD to decide the embedding payload of every two consecutive pixels and embeds secret information bits by adjusting the remainder of the two pixels using the modulus function. M-PVD attains better image quality (increased by 2.5 dB−3.3 dB) compared with Wu and Tsai's PVD method under the same embedding payload.

Chao et al. [13] proposed the DE scheme that relies on pixel pairs as embedding units. In the DE scheme, digits in base B are embedded in pixel pairs, where $B = 2k^2 + 2k + 1$, and $k \geq 1$ is the embedding parameter.Hong et al. [16] proposed an embedding method that adopts the DE scheme in the embedding mechanism. The Hong's proposed method considers the cover local complexity; that is, more secret information is embedded into cover blocks (i.e., pixel pairs) with a complexity greater than a threshold T, and less secret information is embedded into blocks with a complexity less than T. The Hong'sproposed algorithm employs a block adjustment procedure to maintain the consistency of block complexity before and after the embedding process,adding extra distortion to the resulting stego-image.The DE scheme offers high embedding payload while preserving a very acceptable image quality. Although the DE scheme has these advantages, it does not embed different-base digits, which is a vital requirement for any embedding algorithm that considers image quality [16]. This scheme also adds an unacceptable distortion to the image when preventing overflow and underflow problems [17]. Recently, Chen [18] proposed an embedding method that reduces the falling-off-boundary problem that occurs because of the embedding process in cover blocks. The cover image is decomposed into 2 × 2 non-overlapping blocks, denoted as embedding cells. Each embedding cell is decomposed into two embedding units (two pixels in each unit) assigned randomly in a process called embedding arrangement. The difference value d_i of one pair of pixels determines the complexity of the embedding cell.

This paper proposes a new information hiding algorithm to enhance embedding performance in terms of image quality and embedding payload. The proposed algorithm conceals different-base digits in the cover image, instead of embedding single-base digits, to reduce the embedding distortion added to the image because of the embedding process.The rest of the paper is organized as follows: Section 2briefly reviewsthe scheme proposed by Chao et al. Section 3 presents the proposed algorithm. Section 4 discusses the analysis and results of the proposed algorithm. Section 5 presents the steganalysis of the proposed algorithm. Finally, Section 6 presents theconclusions.

II. RELATED WORK

This section reviews the DE scheme proposed by Chao et al. [13]. The DE scheme is exploited as the embedding technique in our proposed algorithm.In the DE scheme, neighboring pixels (p, q) of the cover image are employed as embedding units where digits in base B are embedded, wherein $B = 2k^2 + 2k + 1$, and $k \geq 1$ is the embedding parameter. The DE scheme embeds secret digits by adjusting the pixel pair values. This step changes the difference value for each pixel pair. The maximum embedding payload is equal to $(1/2)\log_2 B$ bit per pixel (bpp) because every two pixels of the stego-image carry $\log_2 B$ bits. The smallest value of the embedding parameter k must be determined when embedding secret information using the following equation:

$$\left\lfloor \frac{M \times N}{2} \log_2 \left(2k^2 + 2k + 1\right) \right\rfloor \geq |S|, \quad (1)$$

where $M \times N$ represents the size of the cover image, and $|S|$ represents the size of the secret information S. A neighborhood set $\varphi(p, q)$ is defined according to Eq. (2)after calculating the embedding parameter k. The diamond characteristic value (DCV) for each pixel pair (a, b) in $\varphi(p, q)$ is computed using Eq. (3).

$$\varphi(p,q) = \{(a,b) | |a-p| + |b-q| \leq k\} \quad (2)$$

$$DCV(a,b) = ((2k+1)a + b) \bmod B \quad (3)$$

The set $\varphi(p, q)$ has two important features. First, no two DCV values are the same.Second,the DCV value of any pixel pair (a, b) is a member of the set $\varphi(p, q)$ and belongs to $\{0, 1, 2, \ldots, B-1\}$. TheDCV values of the set $\varphi(p, q)$ are investigated when embedding secret digit s_B in base B into a pixel pair (p, q) to locate coordinates (p', q'), such that DCV$(p', q') = s_B$. The pixel pair (p, q) is then substituted by (p', q'). To overcome the overflow/underflow problem that can occur, the DE scheme changes p' to p'' and q' to q'' using Eqs. (4) and (5):

$$p'' = \begin{cases} p' - B, & \text{if } p' > 255; \\ p' + B, & \text{if } p' < 0; \end{cases} \quad (4)$$

$$q'' = \begin{cases} q' - B, & \text{if } q' > 255; \\ q' + B, & \text{if } q' < 0; \end{cases} \quad (5)$$

To extract the secret digit s_B embedded in the pixel pair (p', q'), the DCV of (p', q') is calculated; then s_B = DCV(p', q'). A simple example is used to illustrate how the DE scheme works. Suppose that $k = 3$ and a pixel pair $(p, q) = (13, 20)$ is used to embed a digit 6_{25} in base 25. Fig. 1 shows the neighborhood set $\varphi(13, 20)$. Given that DCV(12, 22) = 6 In $\varphi(13, 20)$, the pixel pair (13, 20) is substituted with (12, 22). To extract the embedded digit, the DCV of (12, 22) is then calculated to obtain 6_{25}. Thus, the embedded secret digit is 6_{25}.

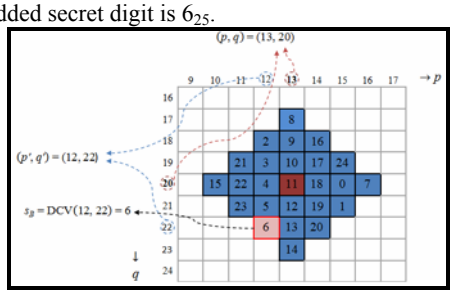

Fig. 1. The neighborhood set $\varphi(13, 20)$, $k = 3$.

III. PROPOSED ALGORITHM

In this section, a new algorithm based on the DE scheme with different-base digits is presented. The DE offers acceptable image quality under various embedding rates, and is secure from LSB steganalysis, such as RS-steganalysis [13]. However, this scheme embeds equal amounts of data into cover pixel pairs, and causes an equal degree of embedding distortion for all embedding places. Moreover, if the embedding of a secret digit into a pixel pair results in an overflow/underflow problem, a pixel value exceeding 255 or 0 is added to (if the pixel value is less than 0) or subtracted from (if the pixel value is greater than 255) the value B to maintain the pixel value within the range [0, 255]. This modification results in large distortion if the embedding parameter, k, is large. For instance, if $k = 4$, then the base B used to hide information is $2 \times 4^2 + 2 \times 4 + 1 = 41$ because$B = 2k^2 + 2k + 1$. However, addition or subtraction of this value leads to large distortion in the stego-image.

This paper presents a new embedding algorithm for digital images based on the DEscheme to improve the embedding efficiency of image steganography in terms of embedding payload and image quality. The proposed algorithm reduces the embedding distortion that occurs in the DE scheme through concealing different-base digits in the cover image. It likewise improves the overflow/underflow strategy used in the DE scheme, thereby removing the unacceptable distortion added to the image.The proposed algorithm is presented in the remaining parts of this section.

A. Secret information division

The proposed algorithm divided the secret information S into two parts, payload P_1 and payload P_2, such that$S = P_1P_2$, where payloadP_1 is embedded into the cover image at a later time using a lower base B_L, and payload P_2 is embedded using a higher base B_H. In other words, two bases (B_L and B_H) are used for the embedding mechanism, where $B_L = 2k_1^2 + 2k_1 + 1$ and $B_H = 2k_2^2 + 2k_2 + 1$, and k_1 and $k_2$are the embedding parameters, such that$k_1 \geq 1$ and $k_2 = k_1 + 1$. Fig. 2 illustrates the relationship between payloads P_1 and P_2 and bases B_L and B_H. The optimum $P_1 – P_2$division must be determined to generate the highest possible image quality for the given secret information.

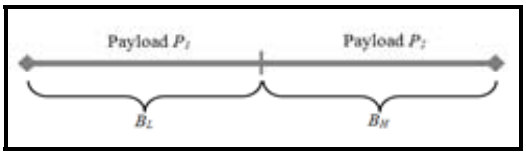

Fig. 2. The relationship between P1 – P2 and bases BL and BH.

To determine the optimal division for P_1 and P_2, theproposed algorithm first calculates the smallest value of parameter k required to embed the entire secret information S. This calculation is conducted by solving the following equation:

$$\left\lfloor \frac{M \times N}{2} \log_2(B) \right\rfloor \geq |S|, \quad (6)$$

where$M \times N$ represents the cover image size, $B = 2k^2 + 2k + 1$, $k_1 \geq 1$, and $|S|$ represents the size of the secret information S. After obtaining the value of k, the values of k_1 and k_2 are determined as follows: If $k > 1$, then the value of k_2 is set to k and the value of k_1 is set to $k_2 – 1$ given that $k_2 = k_1 + 1$. This process produces the two embedding bases B_L and B_H, where $B_L = 2k_1^2 + 2k_1 + 1$ and $B_H = 2k_2^2 + 2k_2 + 1$. However, if $k = 1$, the whole secret information is embedded into the cover image using B_L. After determining the values of k_1 and k_2, the payloads P_1 and P_2 to-be-embedded into the cover image using bases B_L and B_H, respectively, are obtained by solving the following equations:

$$\lfloor |P| \rfloor_1 = \lfloor (M_1 \times N_1)/2 \log$$ (7)

$$|P_2| = |S| - |P_1|, \quad (8)$$

subject to: $$|S| = |P_1| + |P_2|, \quad (9)$$

where$M_1 \leq M$, $N_1 \leq N$,$B_L = 2k_1^2 + 2k_1 + 1$, and $k_1 \geq 1$. Embedding payloads P_1 and P_2 leads to a stego-image with the highest possible image quality for the given secret information by obtaining the maximum values for $M_1$and $N_1$from Eqs. (7-9). For instance, the secret information with size $|S|$ = 305,000 secret bits can be segmented into $|P_1|$ = 303,150 bits and $|P_2|$= 1,850 bits by applying Eqs. (7-9). Although the secret information S can be divided into different $P_1–P_2$divisions, the given division ($|P_1|$ = 303,150 and $|P_2|$= 1,850) leads to the lowest distortion added to the stego-image.After dividing the secret information into two

payloads, P_1 and P_2, the resulting payloads are converted into two sequences of different-base digits. Payload P_1 is converted into a sequence of digits inB_L-ary system, while payload P_2 is converted into a sequence of digits in B_H-ary system. This process produces digits with different bases (D_1 and D_2). After conversion, the resulting D_1 and D_2 sequences are embedded into the pixel pairs of the cover image through the DE schemeusing bases B_L and B_H, respectively.

B. *Adoptingthe DE scheme*

Theconverted digits D_1 and D_2 generated in Section 3.1 are embedded into the pixel pairs of the cover image using the DE scheme. For each digit s_i of theD_1 and D_2 sequences, the DE scheme is used to embed s_i into a pixel pair (p, q) to produce a new pixel pair (p', q') using the corresponding base (B_L for theD_1sequence and $B_H$for theD_2 sequence). At most, one pixel value of the pixel pair (p, q) ischanged to produce (p', q'). If p' or $q'$is out of range [0, 255], the overflow/underflow problem will occur. Applying the same overflow/underflow strategy that used in the DE scheme leads to adding an unacceptable distortion to the stego-image as shown earlier. The proposed algorithm reduces such distortion by identifying an alternative pixel pair (p'', q'') from the pixel pairs surrounding (p, q) to replace (p', q'). As shown in Eq.(3), the alternative pixel pair (p'', q'') satisfies the condition DCV $(p'', q'') = s_i$, where p'' and $q'' \in [0, 255]$. For example, the pixel pair (p, q)= (255, 247) is used to embed the digit $s_i = (0)_5$. Fig.3 shows the neighborhood set $\varphi(255, 247)$. Given that the DCV of (256, 247) in $\varphi(255, 247)$ is equal to 0, the pixel pair (255, 247) is substituted with (256, 247). However, given that the value 256 is out of range [0, 255], an alternative pixel pair is searched from the pixel pairs surrounding (255, 247) to replace (255, 247). The pixel pair (254, 248) has DCV(254, 248) = 0, as shown in Fig. 3. Thus, the pixel pair (255, 247) is replaced by (254, 248). This process continues for all digits of D_1 and D_2 sequences.

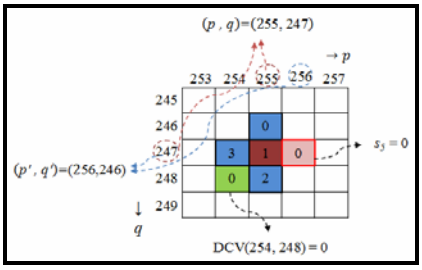

Fig. 3. Neighborhood set φ(255, 247). The alternative pixel pair (254, 248) replaces the pixel pair (255, 247)

C. *Embedding secret information*

Let C be a grayscale image with $M \times N$size, and $S$is the secret information bits with size $|S|$. The embedding places are selected randomly based on a random seed γ. The embedding steps are as follows:

Input: Cover image $C$with size $M \times N$, secret information bits S, and a random seed γ.

Output: Stego-image C'.

Step 1: Divide S into two payloads,$P_1$and P_2, using Eqs. (7-9). The embedding bases $B_L$and B_H are then determined.

Step 2: Convert the bits of the payloads $P_1$and P_2 into two sequences of different-base digits D_1 and D_2 using the embedding bases $B_L$and B_H, respectively.

Step 3: Scan the cover image C from left to right and top to bottom, divide C into 2 × 1 disjointed blocks with pixel pairs (p, q).Usethe random seed γ to randomly generate a sequence of embedding places for the sequences D_1 and D_2.

Step 4: With the corresponding base determined in Step 1 (base B_L for D_1 and base $B_H$for D_2), for each digit s_i of D_1 and D_2, use the DE scheme to embed s_i into a pixel pair (p, q) of the cover image to obtain a new pixel pair (p', q').

Step 5: If p' or $q'$is out of range [0, 255], an alternative pixel pair (p'', q'') is searched from the pixel pairs surrounding (p', q') to replace (p', q') as explained in Section 3.2. Thestego-image $C'$is obtained.

D. *Retrieving secret information*

Once the stego-image C' and embedding parameters such as bases B_L and B_H, size of the payloads P_1 and P_2, size of D_1 and D_2, and random seedγ are obtained, the embedded secret information can be readily retrieved from C'. The retrieving steps are as follows:

Input: Stego-image C', $|P_1|$, $|P_2|$, $|D_1|$, $|D_2|$, B_L, B_H, and random seed γ.

Output: Secret information bits S.

Step 1: Scan the stego-image C' from left to right and top to bottom, divide C' into 2 × 1 disjointed blocks with pixel pair (p, q). Use the random seed γ to generate the same sequence of embedding places that generated during the embedding phase.

Step 2: With the corresponding base (base B_L to extract D_1 and base $B_H$to extract D_2), the DE scheme is used to extract the embedded digits $s_i$from each pixel pair (p, q) used in the embedding. The sequences D_1 and D_2 are obtained.

Step 3: Convert the sequences D_1 and D_2 into two sequences of binary bits. Payloads P_1 and P_2 are then obtained.

Step 4: Obtain the secret message bits S by concatenating the secret bits of $P_1$and P_2; that is, $S = P_1P_2$. The original cover image is evidently not required in extracting the secret message.

E. *A simple example*

Suppose a cover image C is composed of four pixels 55, 56, 62, and 94. Assume also that the secret information bits S to be embedded are $(1110)_2$. During the embedding process, the secret information S is segmented into $|P_1| = 4$ and $|P_2| = 0$ usingEqs. (7-9). Thus, the embedding base $B_L = 5$ is used to embed the payload P_1. Payload P_1 $(1110)_2$ is converted into digits in base-5 becauseB_L= 5,thereby providing theD_1 sequence $(24)_5$. Because $|P_2| = 0$, the D_2 sequence is empty. The cover image C is divided into two pixel pairs: (55, 56) and (62, 94). Assume that embedding occurs in the first pixel pair before the second pixel pair. For the first digit $(4)_5$in D_1, the DE scheme is used to embed $(4)_5$ in the first pixel pair (55, 56) to produce a pixel pair (56, 56), as shown in Fig. 4 (a). Similarly, for the second digit $(2)_5$in D_1, the DE scheme is used to embed $(2)_5$ in the second pixel pair (62, 94) to produce the pixel pair (61, 94), as shown in Fig. 4 (b). All secret information bits are embedded and the embedding process stops. The two pixel pairs (55, 56) and (62, 94) are now changed to (56, 56) and (61, 94), respectively. The stego-image is then obtained.

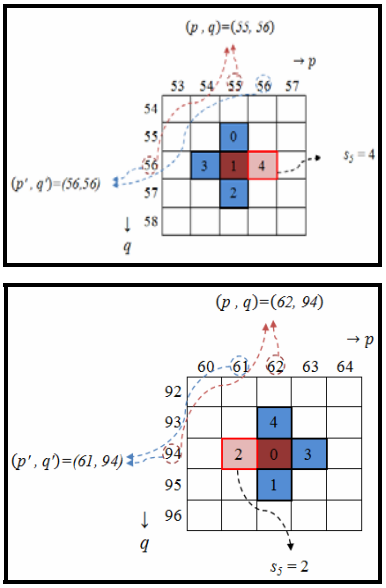

Fig.4. Illustration of the proposed algorithm: (a) the neighborhood set φ(55, 56) for the first pixel pair (55, 56); (b) the neighborhood set φ(62, 94) for the second pixel pair (62, 94).

During the extraction phase, along with the embedding information $|P_1| = 4$, $|P_2| = 0$, $|D_1| = 2$, $|D_2| = 0$, and $B_L = 5$, the secret information can be readily extracted from the stego-image C'. Thestego-image C' is divided into two pixel pairs (56, 56) and (61, 94);$B_L = 5$ is used to extract the secret digits. For the first pixel pair(56, 56), the digit $(4)_5$ is extracted using the DE scheme [Fig. 4 (a)]. Similarly, a digit $(2)_5$ is extracted for the second pixel pair (61, 95) [Fig. 4 (b)]. The two blocks are processed, producing the resulting D_1 digits $(24)_5$. Finally, these digits are converted into binary form to obtain the payload$P_1(1110)_2$.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental results of the proposed algorithm (DE-DBD). Twelve benchmark images were used to evaluate the performance of the proposed algorithm (see Fig. 5). These benchmark images were downloaded from the SIPI [19] and CVG [20] databases. All the test images were grayscale images with a size of 512 × 512. Thesecret informationused in conducting all the experiments was generated by a Pseudo-random Number Generator. Image quality was measured by computing the PSNR. The payload and image quality comparison for the proposed DE-DBD algorithm and the comparisons with the DE scheme and other techniques were also concluded in the experiments. The results are presented in the following subsections.

A. Comparison of payload and image quality

This subsection tests the payload and image quality of resulting stego-images produced by the proposed DE-DBD algorithm. Different payload sizes (low, moderate, and high) were used to conduct the experiments. All 12 images previously mentioned were used to conductthe experiments. Accordingly, the collected results for the used images varied slightly, and the differences between images were negligible. Thus, the effectiveness of the DE-DBD algorithm was not influenced by the number of images used. Table 1 presents the PSNR results for the benchmark images.

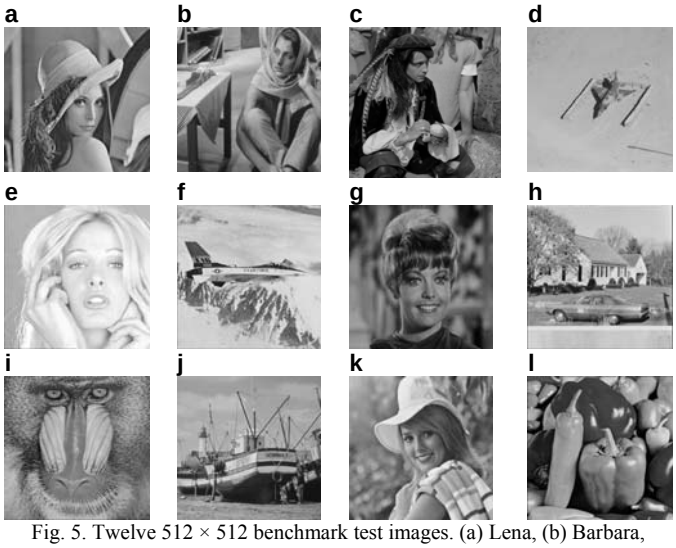

Fig. 5. Twelve 512 × 512 benchmark test images. (a) Lena, (b) Barbara, (c) Man, (d) Airplane, (e) Tiffany, (f) Jet, (g) Zelda, (h)House, (i) Baboon, (j) Boat, (k) Elaine, and (l)Peppers.

TABLE 1. COMPARISON RESULTS OF PSNR WITH DIFFERENT PAYLOADS

Image	Payload 305,000 (B_L–B_H: 5–13)	Payload 500,000 (B_L–B_H: 13–25)	Payload 610,000 (B_L–B_H: 25–41)
	PSNR	PSNR	PSNR
Lena	52.08	47.35	44.89
Barbara	52.07	47.34	44.89
Man	52.06	47.37	44.90
Airplane	52.03	47.32	44.98
Tiffany	52.08	47.37	44.87
Jet	52.07	47.35	44.84
Zelda	52.07	47.35	44.88
House	52.08	47.34	44.95
Baboon	52.07	47.34	44.88
Boat	52.08	47.33	44.90
Elaine	52.07	47.35	44.89
Peppers	52.07	47.36	44.87
Average	**52.07**	**47.35**	**44.89**

Tables 1 show that the proposed DE-DBD algorithm produces stego-images with highly acceptable qualities under various payloads, and the distortions caused by the embedding process are invisible for human perception. Therefore, the DE-DBD algorithm is imperceptible. For instance, the base division B_L–B_H: 5–13 was used to embed the entire payload in the case of low payload. Therefore, the payload was 305,000 bits at 52.07 dB for all images. The base division B_L–B_H: 25–41 was used for the high payload. Therefore, the payload was 610,000 bits at 44.89 dB. This high payload was equivalent to 2.33 bpp. If the test images used in this experiment were embedded by this payload using LSB, the averaged value of PSNR was 39.06 dB. Therefore, using the DE-DBD algorithm results in better image quality compared with the LSB technique.

B. Comparison with the DE Scheme

This subsection tests the payload and image quality of resulting stego-images produced by the proposed DE-DBD algorithm and the DE scheme. Three experiments were conducted to compare the DE-DBD algorithm with the DE scheme. For the payload 305,000, the base division B_L–B_H: 5–13 was used for the DE-DBD algorithm, where the base B = 13 was used for the DE scheme to embed the entire payload. For the payload of 500,000 bits, the base division B_L–B_H: 13–25 was used for the DE-DBD algorithm, where the base B = 25 was used for the DE scheme. In the case of the payload of 610,000 bits, the base division B_L–B_H: 25–41 was set for the DE-DBD algorithm, where the base B = 41 was used for the DE. Thesame test images used in the original paper of the DE scheme [13]were used in this subsection to conduct the experiments. Table 2in Appendix A shows the tabulated comparison results.

Table 2 reveals that the proposed DE-DBD algorithm had higher averaged PSNR value than the DE scheme over 2.06 (= 52.07–50.01) dB when the payload was 305,000 bits. Similarly, the DE-DBD algorithm had higher averaged PSNR values than the DE scheme over 1.59 (= 47.35–45.76) dB and 0.77 (= 44.88–44.11) dB for payloads of 500,000 and 610,000 bits, respectively. These results reveal that the proposed DE-DBD algorithm has better image quality over the DE scheme.

C. Comparison with recent techniques

This subsection presents the comparisons between the proposed DE-DBD algorithm and other approaches. Recent techniques were selected for comparison, namely, M-PVD [15], DE-PVD [16], and PPM-PVD [18]. In comparison with the M-PVD and DE-PVD techniques, the base division for the proposed DE-DBD algorithm was set to B_L–B_H: 13–25. For the M-PVD, six subranges were used to embed the secret message: $R1$ = [0, 7], $R2$ = [8, 15], $R3$ = [16, 31], $R4$ = [32, 63], $R5$ = [64, 127], and $R6$ = [128, 255]. In addition, embedding parameters for the DE-PVD technique were set to k_l = 2, k_h = 3, and T = 4. In comparison with PPM-PVD, the base division for the proposed algorithm was set to B_L–B_H: 25–41, and the embedding parameters for the PPM-PVD technique were set to l = 2, u = 3, and T_0 = 6. Tables 4 to 6 show the results of these experiments. As illustrated in the aforementioned tables,the payload sizes used in the comparison were those closest in each technique. The same set of test images used in each technique was also used in these comparisons.

The comparison results reveal that the averaged PSNR value of the proposed DE-DBD algorithm was5.16 dB higher than that of the M-PVD techniques (Table 3). In addition, the payload of the proposed algorithm was 5,000 bits higher than that of the DE-PVD technique; an increase in averaged PSNR value by 0.44 dB was also observed (Table 4). The proposed DE-DBD algorithm also had a payload that was 1,226 bits higher than that for the PPM-PVD technique, as well as an increase in the averaged PSNR value by 1.35 dB (Table 5). Therefore, the experimental results indicate that the proposed DE-DBD algorithm has better embedding efficiency (i.e., the highest averaged PSNR values) among all the techniques compared at different payload sizes.

TABLE 3. COMPARISON RESULTS OF PSNR OF THE PROPOSED DE-DBD ALGORITHM AND M-PVD

Image	DE-DBD		M-PVD **[15]**	
	Payload	PSNR	Payload	PSNR
Lena	410,000	48.55	409,752	44.10
Airplane	398,000	48.58	397,912	45.20
Boat	422,000	48.42	421,080	42.10
Baboon	458,000	48.05	457,168	40.30
Man	424,000	48.27	423,560	42.10
Tiffany	408,000	48.38	407,360	43.90
Peppers	408,000	48.37	407,256	43.30
Elaine	409,000	48.55	408,592	44.80
Jet	410,000	48.57	409,792	43.50
Average	**416,333**	**48.42**	**415,830**	**43.26**

TABLE 4. COMPARISON RESULTS OF PSNR OF THE PROPOSED DE-DBD ALGORITHM AND DE-PVD

Image	DE-DBD		DE-PVD **[16]**	
	Payload	PSNR	Payload	PSNR
Lena	525,000	46.64	520,000	46.37
Baboon	525,000	46.67	520,000	45.83
Peppers	525,000	46.65	520,000	46.11
Jet	525,000	46.60	520,000	46.55
Boat	525,000	46.68	520,000	46.06
Tiffany	525,000	46.74	520,000	46.41
Barbara	525,000	46.67	520,000	46.12
Zelda	525,000	46.67	520,000	46.42
Average	**525,000**	**46.67**	**520,000**	**46.23**

V. STEGANALYSIS OF THE PROPOSED ALGORITHM

Steganography must evade steganalysis detection. This section shows the experimental results of steganalysis attacks that use the well-known steganalysis RS-steganalysis attack [21] and PVD histogram analysis [22]. RS-steganalysis attack can directly detect the existence of hidden messages in a stego-image. This attack can classify each image pixel under study into regular (R_m, R_{-m}) and singular groups (S_m, S_{-m}). The image passes the RS-steganalysis attack when $R_m \cong R_{-m}$and $S_m \cong S_{-m}$; otherwise, this image reveals the presence of a secret message. The percentage of similarity coefficients for the regular groups, denoted as PSC-RG = ($|R_m - R_{-m}|$)/R_m, and the singular groups, denoted as PSC-SG = ($|S_m - S_{-m}|$)/S_m, were derived to measure the group deviation. Smaller PSC-RG and PSC-SG values indicate that the stego-image is more secure to RS-steganalysis attack.

TABLE 5. COMPARISON RESULTS OF PSNR OF THE PROPOSED DE-DBD ALGORITHM AND PPM-PVD

Image	DE-DBD		PPM-PVD **[18]**	
	Payload	PSNR	Payload	PSNR
Lena	595,000	45.05	593,984	43.70

Boat	637,000	44.14	635,724	42.70
Elaine	641,000	44.08	639,976	42.60
Jet	585,000	45.06	583,132	44.10
House	618,000	44.84	616,708	43.30
Peppers	606,000	44.99	605,036	43.40
Man	626,000	44.60	625,380	42.90
Baboon	700,000	42.83	698,252	41.70
Average	**626,000**	**44.45**	**624,774**	**43.10**

Table 6in Appendix A reports the RS-steganalysis attack results for the proposed DE-DBD algorithm. This experiment was conducted using four images. The results for the other images were relatively similar.The statistics in Table 6 reveal that the PSC-RG and PSC-SG values obtained by the proposed algorithm were close to 0. Thus, the RS-steganalysis attack failed to detect the DE-DBD algorithm.

The DE-DBD algorithm was also tested by PVD histogram analysis. Fig.6 shows the PVD histogram results for only two of the images because of the extreme similarity in analysis results for the 12test images. The images "Lena," and "Peppers" were used in these experiments. If the PVD histogram does not display a smooth curve, the image is considered suspicious. Based on the experimental results shown in Fig.6, the DE-DBD algorithm was undetectable by the PVD histogram analysis. Therefore, the DE-DBD algorithm is secure against the RS-steganalysis and PVD histogram analysis attacks.

LenaPeppers

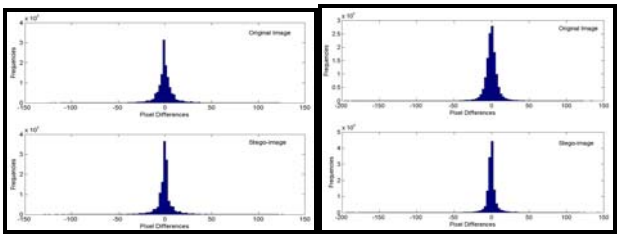

Fig. 6. PVD histogram analysis for two test images and corresponding stego-images.

VI. CONCLUSION

This paper proposed an efficient information embedding algorithm based on the DE scheme with different-base digits. The proposed algorithm divides the secret information into two payloads, and then embeds each payload into the cover image using a different base. The main contributions of the proposed algorithm are: (1) The proposed algorithm reduces the embedding distortion that occurs in the DE scheme by concealing different-base digits in the cover image instead of concealing single-base digits. (2) The proposed algorithm improves the overflow/underflow strategy used in the DE scheme, therebyreducing the distortion added to the image to solve the overflow/underflow problem.(3) The proposed algorithm enhances the embedding performance compared with other state-of-art embedding techniques, and is robust against recent steganalysis attacks, such as RS-steganalysis and PVD histogram analysis. The experimental results revealed that the proposed algorithm hasbetter embedding efficiencycompared with other techniques in terms of image quality and embedding payload.

REFERENCES

[1] Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in Digital Images: Common Approaches and Tools. *IETE Technical Review, 30*(4), 344-358.

[2] Al-Dmour, H., & Al-Ani, A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert Systems with Applications, 46*, 293-306.

[3] Das, S., Bandyopadhyay, B., & Sanyal, S. (2008). Steganography and Steganalysis: different approaches. *Information Technology and Engineering (IJCITAE), 2*(1), 1-11.

[4] Kanso, A., & Own, H. S. (2012). Steganographic algorithm based on a chaotic map. *Communications in Nonlinear Science and Numerical Simulation, 17*(8), 3287–3302.

[5] Ingemar, J. C., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography* (2 ed.). USA: Burlington, Morgan Kaufmann.

[6] Al-Ani, Z. K., Zaidan, A., Zaidan, B., & Alanazi, H. (2010). Overview: Main fundamentals for steganography. *Journal of Computing, 2*(3), 158-165.

[7] Lin, E. T., & Delp, E. J. (1999, 25–28 April 1999). *A review of data hiding in digital images.* Paper presented at the Proceedings of the Image Processing, ImageQuality, Image Capture Systems Conference (PICS'99), Georgia, USA.

[8] Atawneh, S., & Sumari, P. (2014). Imperceptible image-based steganographic scheme using Bit-Plane Complexity Segmentation (BPCS). *International Journal of Image Processing Techniques, 1*, 6 - 11.

[9] Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142-172.

[10] Chan, C.-K., & Cheng, L.-M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*(3), 469-474.

[11] Saleh, N. A., Boghdady, H. N., Shaheen, S. I., & Darwish, A. M. (2010). High capacity lossless data embedding technique for palette images based on histogram analysis. *Digital Signal Processing, 20*(6), 1629-1636.

[12] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*(9), 1613-1626.

[13] Chao, R. M., Wu, H. C., Lee, C. C., & Chu, Y. P. (2009). A novel image data hiding scheme with diamond encoding. *EURASIP Journal on Information Security, 2009*(1), 1-9.

[14] Sun, S. (2016). A novel edge based image steganography with 2 k correction and Huffman encoding. *Information Processing Letters, 116*(2), 93-99.

[15] Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software, 81*(1), 150-158.

[16] Hong, W., Chen, T. S., & Luo, C. W. (2012). Data embedding using pixel value differencing and diamond encoding with multiple-base notational system. *Journal of Systems and Software, 85*(5), 1166-1175.

[17] Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., & Gupta, B. (2016). Secure and imperceptible digital image Steganographic algorithm based on diamond encoding in DWT domain. *Multimedia Tools and Applications*, 1-22.

[18] Chen, J. (2014). A PVD-based Data Hiding Method with Histogram Preserving Using Pixel Pair Matching. *Signal Processing: Image Communication, 000*(000), 000-000.

[19] USC. USC-SIPI image database Retrieved 16-January, 2013, from http://sipi.usc.edu/database/

[20] CVG. CVG image database Retrieved 5-April, 2014, from http://decsai.ugr.es/cvg/dbimagenes/g512.php

[21] Fridrich, J., & Goljan, M. (2004). USA Patent No.: U. S. Patent.

[22] Zhang, X., & Wang, S. (2004). Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. *Pattern Recognition Letters, 25*(3), 331-339.

Appendix A

TABLE 2. COMPARISON RESULTS OF PSNR OF THE DE-DBD ALGORITHM AND DE USING VARIOUS PAYLOADS

Image	Payload = 305,000 bits		Payload = 500,000 bits		Payload = 610,000 bits	
	DE-DBD	DE	DE-DBD	DE	DE-DBD	DE
Lena	52.08	49.99	47.35	45.77	44.89	44.11
Jet	52.07	50.00	47.35	45.72	44.84	44.10
Boat	52.08	50.02	47.33	45.76	44.90	44.12
Tiffany	52.08	50.04	47.37	45.77	44.87	44.09
Peppers	52.07	49.99	47.36	45.76	44.87	44.10
Baboon	52.07	50.02	47.34	45.78	44.88	44.11
Barbara	52.07	50.02	47.34	45.75	44.89	44.10
Zelda	52.07	50.02	47.35	45.77	44.88	44.12
Average	**52.07**	**50.01**	**47.35**	**45.76**	**44.88**	**44.11**

TABLE 6. STATISTICS OF RS-STEGANALYSIS ATTACK FOR 4 STEGO-IMAGES EMBEDDED BY 305,000 BITS

Image	R_m	R_{-m}	S_m	S_{-m}	PSC-RG	PSC-SG
Lena	32421	32434	17589	17768	0.0004	0.0102
Peppers	32461	32529	16985	17007	0.0021	0.0013
Baboon	32844	32776	27865	27863	0.0021	0.0001
House	28940	28758	17222	17329	0.0063	0.0062