Journal of Computer and Communications, 2021, 9, 70-87
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Block Mean Insertion and Dual Stego Generation Based Embedding Strategy

Md. Habibur Rahman[1], A. H. M. Kamal[2]

[1]Dept. Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh
[2]Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh
Email: shawoncsebd@gmail.com, kamal@jkkniu.edu.bd

How to cite this paper: Rahman, Md.H. and Kamal, A.H.M. (2021) A Block Mean Insertion and Dual Stego Generation Based Embedding Strategy. *Journal of Computer and Communications*, **9**, 70-87.
https://doi.org/10.4236/jcc.2021.93005

Received: February 1, 2021
Accepted: March 19, 2021
Published: March 22, 2021

Abstract

In reversible data hiding, pixel value ordering is an up-to-the-minute research idea in the field of data hiding. Secret messages are embedded in the maximum or the minimum value among the pixels in a block. Pixel value ordering helps identify the embeddable pixels in a block but suffers from fewer embedding payloads. It leaves many pixels in a block without implanting any bits there. The proposed scheme in this paper resolved that problem by allowing every pixel to conceive data bits. The method partitioned the image pixels in blocks of size two. In each block, it first orders these two pixels and then measures the average value. The average value is placed in the middle of these two pixels. Thus, the scheme extends the block size from two to three. After applying the embedding method of Weng *et al.*, the implantation task removed the average value from the block to reduce its size again to two. These two alive pixels are called stego pixels, which produced a stego image. A piece of state information is produced during implanting to track whether a change is happening to the block's cover pixels. This way, after embedding in all blocks, a binary stream of state information is produced, which has later been converted to decimal values. Thus, image data were assembled in a two-dimensional array. Considering the array as another image plane, Weng *et al.*'s method is again applied to embed further to produce another stego image. Model validation ensured that the proposed method performed better than previous work in this field.

Keywords

Reversible Data Hiding, Stego Image, Multilayer Embedding, Block Partition, Embedding Payload

1. Introduction

The modern era begins to embrace data security as an important issue for data science; thus, the researcher concentrates on data hiding for two decades [1]. Data Hiding is a technique by which it can embed secret data into a cover medium where the desired user can extract the embedded data from the marked medium for various purposes [2]. That's why data hiding has become a hot research topic, especially for the research community increasingly being used in forensic, medical, military, satellite applications, industrial control units [3] [4].

Data hiding is a fundamental part of steganography and watermarking [1]. The hiding of secret information is accomplished by watermarking or steganography, which is a technique that embeds secret data into multimedia (like image, video, text, audio) that can be visible or invisible. A printed watermark is a visible watermark (like compass stamp watermarking), whereas a digital watermark is an invisible watermark (like audio clips). Visible and invisible watermarking is used to protect the owner's ownership [5]. To hide a secret message into a multimedia carrier, e.g., video, audio, images for different applications, including content authentication, copyright protection, forensic report management, satellite application, etc., is a challenging task [6] [7] [8]. There are two steganographic methodologies, *i.e.*, reversible and irreversible methods. The irreversible method extracts the stego image from the cover image without extracting the cover image in the receiver end [9] [10] [11] [12] [13]. But the reversible data hiding methods retrieve not only secret data but also cover images from the stego image. The irreversible data hiding is inefficient when both embedded data and cover image are required. The reversible data hiding (RDH) paves the way to retrieve both secret data and cover one. For conducting reversibility, in the data embedment process, these schemes inlay extra information. Under those circumstances, the original embedding capacity will decrease and increase the processing complexity. As has been noted, reversible data hiding increases the security of the message and the robustness of the algorithm. In essence, an intruder cannot identify and understand the hidden information [14].

Reversible data hiding algorithms have been classified into several categories: RDH into special image domain, encrypted images, video and audio, contrast enhancement, compressed domain, semi-fragile authentication [15]. To perform the reversible data hiding scheme, there are two technical issues, *i.e.*, 1) pixel difference/ reference pixel and 2) multilayer embedding. Here, pixel difference can be performed by subtraction from reference pixel to neighbors, which are pre-assigned where histogram shifting plays a great role here, which is used to prevent overflow and underflow. Message bits are embedded by not only histogram shifting but also expanding the contents in the embedding spaces. Hence, after completing difference histogram shifting, for improving hiding capacity, multilayer embedding is used to embed huge data and decrease noise. Recovery of the original object from the stego image is a demand of data hiding scenario after the secret information is extracted. High-capacity steganography using multilayer embedding (CRS) can enhance the performance of an information hiding system. After ensuring high capacity, the process of maximizing the difference values between neighboring pixels is applicable to information hiding and reversible data hiding method [16]. In previous work, there is a critic which is irreversible presented in centralized difference expansion scheme. They try to improve this problem and assure reversible criteria [17]. Moreover, in reversible data hiding, interpolation is a part of image processing where efficient interpolation can increase payload. Among different interpolation methods, *i.e.*, NMI, NNI, and BI, Xian-ting Zeng *et al.*'s scheme promotes the performance of data hiding schema where Interpolation by Neighboring Pixels (INP) was used to decrease false colors and zipper effects [18]. Whereas Huang *et al.*'s. Scheme improved payload up to 56% to 108% while minimizing image distortion as well. Histogram Association Mapped is another idea in reversible data hiding. To enhance the robustness of visual degradation based HAM, Habiba *et al.*'s scheme worked in this field [19]. In the reversible data hiding arena, seven levels of security features are a new invention. Kamal *et al.*'s used seven levels of security in an encapsulation way [20].

Previous researches work on improving embedding capacity through various techniques. A binary tree is introduced by Wei-Liang *et al.*'s for improving embedding capacity through histogram by the adjacent pixels [21]. Jiann-Der Lee *et al.*'*s* used side-match vector quantization technique (SMVQ) to reconstruct the cover image, which yields a higher embedding capacity [22]. Besides, Mingwei Tang *et al.*'s introduced the image steganography truncation and interpolation (AMBTC) technique used to increase the embedding capacity and image quality [23]. Steganalysis algorithm is used to detect the stego images. Many authors work in this field. Hedieh Sajedi *et al.*'s was one of them [24]. Whereas, the multi-threshold based audio steganography scheme was introduced by Dulal C. Kar *et al.*'s [25]. In Dulal C. Kar *et al.*'s scheme detection of the stego audio cannot be performed by an intruder which played a great role in audio steganography. To enhance the embedding capacity, Kamal *et al.*'s try to rise the embeddable error using multi predictors where the optimal prediction error is extracted from the combination of multi predictors and hybrid errors [4]. As a matter of fact, achieving high image fidelity at the low payload is another new research field in Reversible Data Hiding [26]-[32] arena. Li *et al.*'s work paves the way for pixel value ordering (PVO) [33]. Peng *et al.*'s proposed an improved PVO (IPVO) method. The new difference is calculated from the pixel locations of the maximum and second-largest values (similarly, the minimum and second smallest values). In that case, embeddable prediction-errors are hugely raised. Li *et al.*'s work is promoted by Peng *et al.*'s work [27]. Peng *et al.*'s used threshold values. At the same time, complexity measurement is also calculated by this scheme.

Embedding capacity depends on threshold values and complexity measurement. To improve the embedment process, Wang *et al.*'s scheme is improved by Weng *et al.*'s methodology [34]. Improvement is made by considering unequal blocks. In partition and modification of a block, Weng *et al.*'s considered smooth, normal & flat blocks. Complexity measurement helps to make a decision whether the block is a rough, normal, or flat block. Complexity measurement helps to divide the block into sub-blocks. The lower the complexity level, the smaller the sub-blocks. At the same time, data embedment will be increased. Similarly, if the complexity level is high, the size of the sub-block will be large. And as a result, data embedment will be decreased. The dynamic block strategy of Wang *et al.*'s did not have enough embedding capacity [34]. Wenguang He *et al.*'s worked in this field [35]. To overcome the problem of lower data embedment, Wenguang He *et al.*'s proposed multistage blocking [35].

The research field in RDH focuses on achieving high image fidelity at the low payload. Hence, this article's main goal is to enhance the embedding capacity by block mean insertion techniques where a dual stego image would be created. In all the PVO-based schemes, stated in the preceding sections, the quantity of the embedded bits, also known as payload, depends on pixel modification in the process of data embedment. The difference between the maximum and second maximum (or minimum and second minimum) predicts the possibility of data embedding. If the pixel block size is small, data embedding capacity will be dramatically increased.

The remaining parts of this article are organized into four more chapters. Chapter 2 illustrates the proposed methodology based on the related works on which the proposed work builds its basement. Chapter 3 delineates the experimental results and discussion over the competing schemes. Finally, chapter 4 concludes the article.

2. Methodology

The proposed scheme takes a cover image I of size $x \times y$. Each pixel at (i, j) location of the image is read by $I_{i,j}$. The proposed scheme implants the secrets in the contents of $I_{i,j}$. The data implantation method generates two stego images, say S_1 and S_2.

For instance, pixel p_1 and pixel p_2 are situated in two neighbor positions in image I. These two pixels are used to generate a third-pixel p_a. The p_a is the average value of p_1 and p_2. The pixel values and the average value are arranged in the order of p_1, p_a, and p_2. The proposed method applies Weng *et al.'s* data embedding algorithm in the values of p_1, p_a, and p_2. After the data implantation task, the embedding algorithm produces three modified pixels p_1', p_a', and p_2' are produced. These two stego pixels p_1' and p_2' are placed in an image grid of I's size at the same positions as p_1 and p_2 are located in I. The whole embedding process is executed for each other neighboring pair. The process finally produces a stego image S_1 from I. The embedding algorithm may change the value of p_1 and p_2 depending on the value of to-be implanted bits and the value of $d_{1\max}$ and $d_{2\max}$. While implanting data, the embedding method keeps track of changes in p_1 and p_2 by state values. A "0" as a state value means that the value of p_1 has not been modified. On the other saying, a "1" means that the value of p_1 has been changed. Thus, the scheme generates $(x * y)/2$ number of state information for an image of size $x \times y$ for p_1 only. Similarly, it engenders $(x * y)/2$ bits as state information for p_2. Thus, the total length of state information is $x \times y$ bits. Every 8 bits of $x \times y$ binaries are converted to a decimal value. The number of decimal values will be $(x * y)/8$, where each value range will be [0, 255]. If we arrange these 0 to 255 ranged values in a two-dimensional array F, the F will act as another image plane. The decoder end will require the binary values, *i.e.*, state information, to reconstruct the cover pixels. Though one can send that F as a side-information to the destination through another communication channel to help reconstruct the original, it will be better to apply a reversible algorithm to implant more data bits in F when the demanding payload is high. This will also increase the security as F's contents will be changed in the stego of F. In this study, authors applied the scheme of Weng *et al.*'*s* [34]. The method generated a stego image S_2 for F.

In **Figure 1**, pixel values are $p_1 = 148$, $p_2 = 149$, $p_a = 149$. The p_a is created by averaging the value of p_1 and p_2. A difference between p_2 and p_a is measured by $p_a - p_2$. Say the difference value is $d_{1\max}$. Similarly, another $d_{2\max}$ is computed from $p_1 - p_2$. According to Weng *et al.*'s [34] data implantation method, the stego value of p_2 will be p_2'. To explain the scenario, again consider the pixel values in **Figure 1**. Here, $p_1 = 148$, $p_2 = 149$, $p_a = 149$. These values yield that $d_{1\max} = 0$. While implanting a secret bit b = 1 by the data implantation method of Weng *et al.*'*s* [34], as of **Table 1**, in pixel p_2, the value of p_2 will be modified by $p_2' = 150$.

Both stego one and stego two were sent to the receiver end. The receiver extracts hidden data from these stego images. To extract the data from S_1, the receiver has to reconstruct the F from the stego S_2, first because F carries the state information, which is required to reconstruct I from S_1. The extraction of data and reconstruction of original F from the stego image, S_2, is well explained in Weng *et al.*'*s* scheme. Therefore, Weng *et al.*'*s* scheme will give us F along with the extracted data from S_2. The binary conversion of F will provide us the state information. These state information are used in extracting the secrets from S_1 as well as to rebuild the cover image I. Here, the process of rebuilding I involved two steps: first, data extraction from stego two; second, gray-scale image to binary image conversion. Authors applied Weng *et al.*'*s* extraction algorithm both in stego two and stego one to extract data.

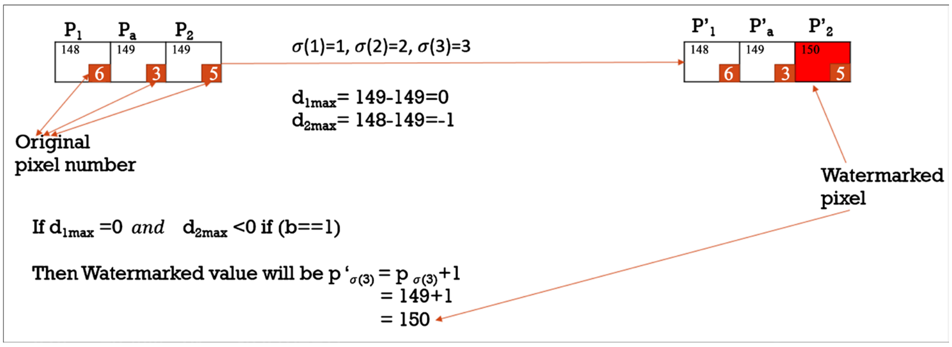

Figure 1. Stego creation strategy.

Table 1. Embedment condition and values.

Conditions on ($d_{1\max}$, $d_{2\max}$)		Embedded values

$d_{1\max}=1$ and $d_{2\max}=0$	$d_{1\max}=1$ or $d_{2\max}=0$	if (b1 == 0 and b2 == 0)
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}$
		else if (b1 == 0 and b2 == 1)
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}-1, P'_{\sigma(3)}=P_{\sigma(3)}$
		else if (b1 == 1and b2 == 0)
		$P'_{\sigma(2)}=P_{\sigma(2)}-1, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}$
		else if (b1 == 1and b2 == 1
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}+1$

	$d_{1\max}>1$ or $d_{2\max}<0$	if (b1 == 1)
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}+1$
		else if (b1 == 0)
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}-1, P'_{\sigma(3)}=P_{\sigma(3)}$

$d_{1\max}\in(-\infty,-1]\cup[2,\infty)$	$d_{2\max}=0$ and $d_{2\max}=0$	if (b1 == 1)
		$P'_{\sigma(2)}=P_{\sigma(2)}, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}+1$
		else if(b1 == 0)
		$P'_{\sigma(2)}=P_{\sigma(2)}-1, P'_{\sigma(1)}=P_{\sigma(1)}, P'_{\sigma(3)}=P_{\sigma(3)}$

	$d_{1\max}\in(-\infty,-1]\cup[2,\infty)$	$P'_{\sigma(3)}=P_{\sigma(3)}+1$

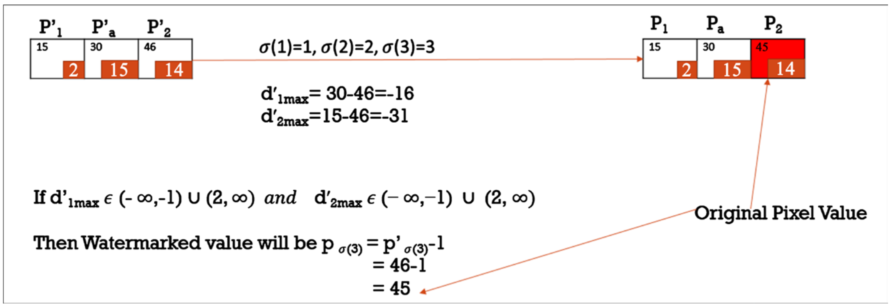

Figure 2. Stego two extraction strategy.

In Figure 2 pixels $p'_1=15$, $p'_2=46$, $p'_a=30$. Pixel p'_2 is created from the mean value of pixels p'_1 and p'_2. There are two differences created. The first one is $d'_{1\max}$, and the second one is $d'_{2\max}$. The $d'_{1\max}$ is created from the subtraction operation of p'_a and p'_2. From Figure 2, $p'_a=30$ and $p'_2=45$. So, $d'_{1\max}=p'_a-p'_2=30-46=-16$. On the other hand, $p'_1=15$ and $p'_2=45$. So, $d'_{2\max}=p'_1-p'_2=315-46=-31$. The watermarked value will be p_2 = 45. However, $p_1=p'_1$, $p_a=p'_a$. Now the gray-scale value is retrieved.

In Figure 3 pixels $p'_1=148$, $p'_2=149$, $p'_a=150$. Pixel p'_a is created from the mean value of pixels p'_1 and p'_2. There are two differences created. The first one is $d'_{1\max}$, and the second one is $d'_{2\max}$. The $d'_{1\max}$ is created from the subtraction operation of p'_a and p'_2. From Figure 3 $p'_a=150$ and $p'_2=149$. So, $d'_{1\max}=p'_a-p'_2=149-150=-1$. On the other hand, $p'_1=148$ and $p'_2=150$.

So, $d'_{2\max} = p'_1 - p'_2 = 148 - 150 = -2$. The watermarked value will be p_2 = 149. However, $p_1 = p'_1$, $p_a = p'_a$. Now we get the gray-scale value. From Table 2, extracted bit information or hidden data were generated. Also original image pixel was retrieved, which is similar to the cover image.

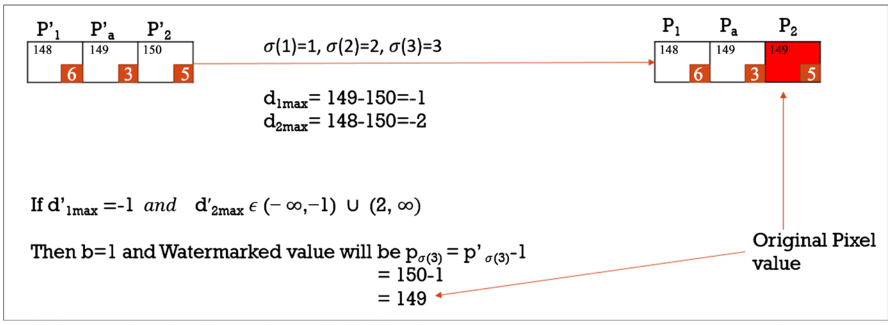

Figure 3. Stego one extraction strategy.

Table 2. Data extraction table.

Conditions on ($d'_{1\max}$, $d'_{2\max}$)	Extracted values	
$d'_{1\max} = 1$ and $d'_{2\max} = 0$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 0
$d'_{1\max} = 0$ and $d'_{2\max} = 1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 0
$d'_{1\max} = 0$ and $d'_{2\max} = 0$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 0
$d'_{1\max} = 1$ and $d'_{2\max} = 1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 0
$d'_{2\max} = 2$ and $d'_{2\max} = 2$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1 and b2 = 1
$d'_{1\max} = 2$ and $d'_{2\max} = -1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1 and b2 = 1
$d'_{1\max} = -1$ and $d'_{2\max} = -1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1 and b2 = 1
$d'_{1\max} = -1$ and $d'_{2\max} = 2$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1 and b2 = 1
$d'_{1\max} = 2$ and $d'_{2\max} = 1$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 1 and b2 = 0
$d'_{1\max} = 2$ and $d'_{2\max} = 0$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 1 and b2 = 0
$d'_{1\max} = -1$ and $d'_{2\max} = 1$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 1 and b2 = 0
$d'_{1\max} = -1$ and $d'_{2\max} = 0$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 1 and b2 = 0
$d'_{1\max} = 1$ and $d'_{2\max} = -1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 1
$d'_{1\max} = 1$ and $d'_{2\max} = 2$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 1
$d'_{1\max} = 0$ and $d'_{2\max} = 2$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 1
$d'_{1\max} = 0$ and $d'_{2\max} = -1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0 and b2 = 1
$d'_{1\max} = 1$ and $d'_{2\max} \in (-\infty, -1) \cup (2, \infty)$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0
$d'_{1\max} = 0$ and $d'_{2\max} \in (-\infty, -1) \cup (2, \infty)$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)} + 1, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0
$d'_{1\max} = 2$ and $d'_{2\max} \in (-\infty, -1) \cup (2, \infty)$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1

Continued

$d'_{1\max} = -1$ and $d'_{2\max} \in (-\infty,-1)\cup(2,\infty)$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1
$d'_{1\max} \in (-\infty,-1)\cup(2,\infty)$ and $d'_{2\max} \in (-\infty,-1)\cup(2,\infty)$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	no embedded data bit
$d'_{1\max} \in (-\infty,-1)\cup(2,\infty)$ and $d'_{2\max} = 1$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0
$d'_{1\max} \in (-\infty,-1)\cup(2,\infty)$ and $d'_{2\max} = 0$	$P_{\sigma(2)} = P'_{\sigma(2)} + 1, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)}$	b1 = 0
$d'_{1\max} \in (-\infty,-1)\cup(2,\infty)$ and $d'_{2\max} = 2$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1
$d'_{1\max} \in (-\infty,-1)\cup(2,\infty)$ and $d'_{2\max} = -1$	$P_{\sigma(2)} = P'_{\sigma(2)}, P_{\sigma(1)} = P'_{\sigma(1)}, P_{\sigma(3)} = P'_{\sigma(3)} - 1$	b1 = 1

Experimentally it is observed that the embedding payloads are higher than the schemes reviewed in the literature. The proposed scheme achieves higher embedding capacity than Peng *et al.'s* [27], Wang *et al.'s* [30] and Weng *et al.'s* method [34]. The simulation results demonstrate that the embedding capacity is improved notably compared with its competing scheme. Additionally, this scheme improves the stego image quality.

3. Experimental Results and Discussions

The study conducted experiments on 499 images, which were collected from the USC-SIPI dataset, the BOSS image dataset, online newspapers, and various research sites. The images were resized to 510 × 510. For the convenience of presentations, the numerical results of only ten images of **Figure 4** are shown here, although the proposed scheme resolved the observations in all the experimented images. The proposed method is appraised by comparing its results with Peng *et al.'s* method [27], Wang *et al.'s* method [30], and Weng *et al.'s* method [34]. The embedding payload, the peak signal to noise ratio (PSNR), the standard deviation peak signal to noise ratio (PSNR), the standard deviation, and the entropy were analyzed in the experiments. The demonstrated results justify the claim of boosting up the embedding payload and improving the distortions in the image quality by the proposed scheme.

3.1. Analysis of Embedding Payloads

The experimental results showed in **Figure 5** indicate that the proposed scheme noticeably dominates the others by the achieved payload. The payload of the first 100 images of the Miscellaneous, Textures, Sequences image dataset is depicted along the y-axis. Among the compared schemes, Peng *et al.'s* presented low embedding payloads because, in this method, only a single bit of information is planted in each block, whereas the proposed method embeds more payloads than Peng *et al.'s* method. The proposed scheme also outperforms Wang *et al.'s* method as the author used thresholding and complexity measurement for which the number of embedded bits is less. The data embedment also depends on block partitioning. Wang *et al.'s* use a 4 × 4 block to embeds data. A good number of blocks cannot conceive data only for the threshold mismatching. On the other

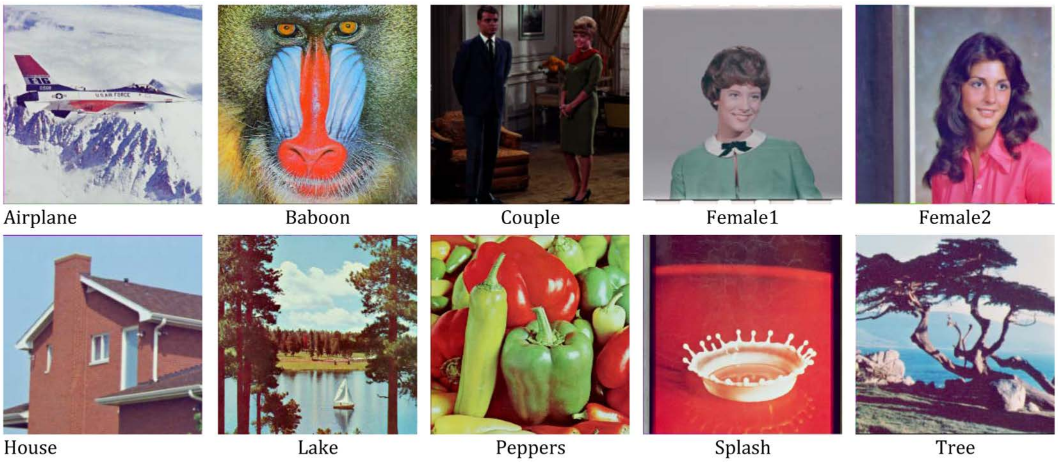

Figure 4. Sample of 10 images taken from USC-SIPI.

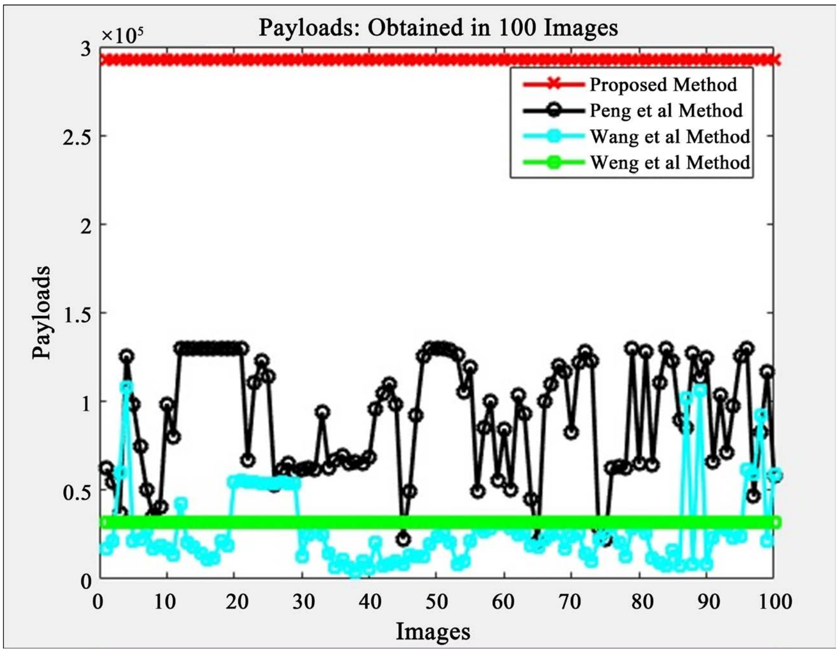

Figure 5. Comparison of payloads achieved in the first 100 images of USC-SIPI.

hand, if a block's complexity does not match the requirement of data embedment, there will be no chance of data embedment. Even for thresholding uses, sometimes Peng *et al.'s* scheme outperforms Wang *et al.'s* method.

Weng *et al.'s* method embeds fewer number payloads than the proposed method. In **Figure 6**, the green color line represents the payload capacity. Two thresholds and one variance are calculated in Weng *et al.'s* method. Variance is calculated from the rightmost and lowermost regions of a block. Block partition and block modification are dependent on the variance value. The author takes a range of variance values. As a result, some pixel blocks are changed, and some others are not changed. Payload embedment is dependent on block modification. On the contrary, threshold values and variance are not considered in the proposed method. So, data embedment is higher than Weng *et al.'s* method.

Figure 6 shows that Weng *et al.*'*s* method embeds a lower payload than the proposed method.

The experimental results of sample 10 images demonstrate that the proposed scheme outperforms over competitive works. Figure 6 shows the payload number on the y-axis and images on the x-axis. So Table 3 clearly demonstrates that the proposed scheme carries a higher payload than Peng *et al.*'*s*, Wang *et al.*'*s*, and Weng *et al.*'*s* scheme.

Hence, the embedding payload in the proposed scheme is much higher than the obtained payload in Peng *et al.*'s scheme. The embedding payload is higher

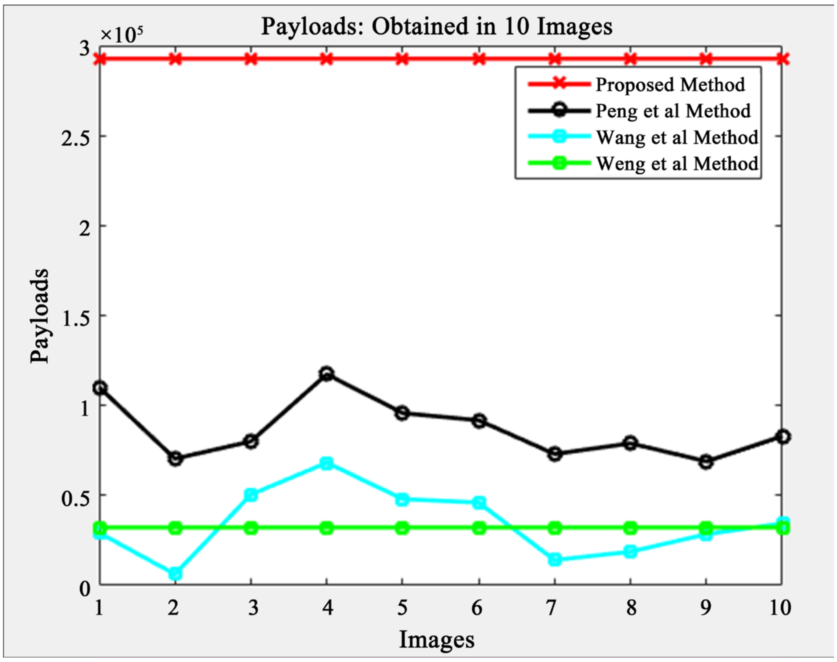

Figure 6. Comparison of payloads achieved from sample 10 images.

Table 3. Comparison of payloads in different schemes for sample 10 images with proposed one.

Images Name	Peng *et al.*	Wang *et al.*	Weng *et al.*	Proposed
Airplane.tiff	110,204	29,291	32,258	292,744
Baboon.tiff	70,422	6236	32,258	292,744
Couple.tiff	80,024	50,497	32,258	292,744
Female1.tiff	117,364	68,186	32,258	292,744
Female2.tiff	95,754	47,991	32,258	292,744
House.tiff	91,757	46,066	32,258	292,744
Lake.tiff	73,033	14,101	32,258	292,744
Peppers.tiff	78,967	18,743	32,258	292,744
Splash.tiff	68,938	28,485	32,258	292,744
Tree.tiff	82,918	34,464	32,258	292,744
Average	**86,938.1**	**34,406**	**32,258**	**292,744**

than both Wang *et al.*'s method and Weng *et al.*'s method. As a concluding remark, it can be said that the proposed scheme certainly enhances the embedding payload.

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

3.2. Analysis of PSNR

The target of the proposed scheme is to increase the embedding capacity. We embed more bits in various block sizes (e.g., 1 × 3 blocks, 2 × 2 blocks, 4 × 4 blocks). The proposed method considers a 1 × 2 size block to embed the payload. Peng *et al.'s* considered a 2 × 2 block. Hence, in the experiment, both for 1 × 2 and 2 × 2 image blocks were taken. To test statistically, the PSNR of the resulted stego images are measured by the following Equation (1)-

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \tag{1}$$

$$\text{MSE} = \frac{\sum_{i=1}^{\text{row\_size}}\sum_{j=1}^{\text{column\_size}}\left(I_{i,j} - \tilde{I}_{i,j}\right)^2}{\text{row\_size} * \text{column\_size}} \tag{2}$$

where MSE stands for mean-square-errors and MSE is measured by the following Equation (2)-

In Equation (2), $I_{i,j}$ is the cover image and $\tilde{I}_{i,j}$ is a stego image. Row size is the height of images, and Column size is the width of images.

For the convenience of presentations, the pictorial representation of PSNR is illustrated in **Figure 7** for only ten images, although the proposed scheme resolved the observations in all the experimented images. The proposed method gives lower PSNR than the Weng *et al.'s* method, Wang *et al.'s* method, and Peng *et al.'s* method. Nevertheless, the number of embedded bits of the proposed method is higher than the one by the Weng *et al.'s* method, Peng *et al.'s* method, and Wang *et al.'s* method.

Although the competing works give better PSNR, these methods do not carry a higher embedding payload than the proposed method. From **Table 4**, it is being observed that the proposed method gives higher payloads than the competing works. Hence, it can be inferred that the proposed scheme outperforms Peng *et al.'s* method [27], Wang *et al.'s* method [30], and Weng *et al.'s* method [34].

3.3. Steganalysis

Steganalysis is an experiment to detect hidden information from an image. Researchers, encroachers, intelligent devices can detect hidden information by checking the resistance of stego images. Statistical analysis plays a great role here. Standard deviation and entropy are the statistical analyzers. By using standard deviation, an intruder can measure the resistance of stego images. The

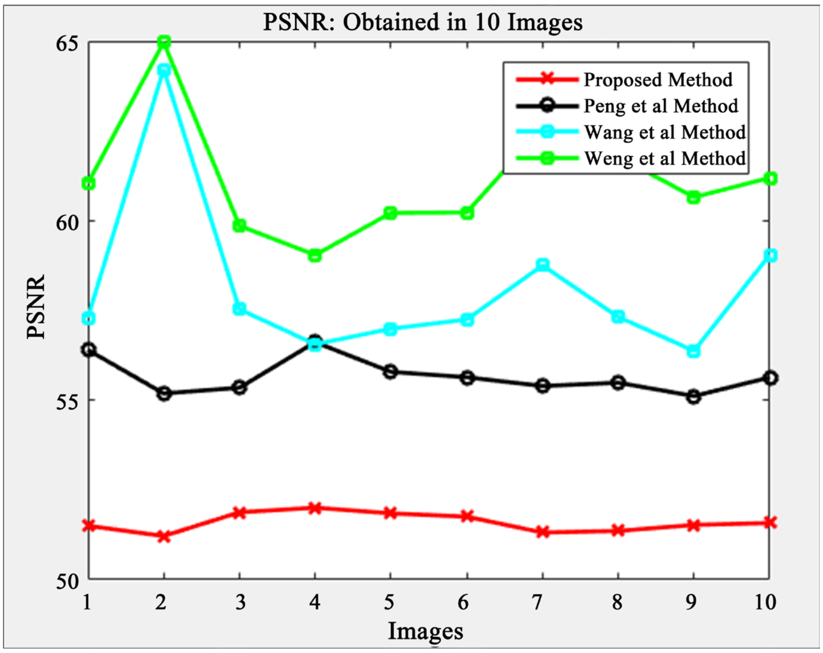

Figure 7. Comparison of PSNR among different schemes.

Table 4. Comparison of payloads per PSNR with proposed one.

Images Name	In Peng *et al.*	In Wang *et al.*	In Weng *et al.*	In Proposed
Airplane.tiff	1953.97	1953.97	528.46	5684.08
Baboon.tiff	1276.06	1276.06	496.53	5715.87
Couple.tiff	1445.88	1445.88	538.91	5643.03
Female1.tiff	2073.08	2073.07	546.35	5629.12
Female2.tiff	1716.36	1716.36	535.72	5646.23
House.tiff	1649.19	1649.19	535.60	5656.25
Lake.tiff	1318.42	1318.42	515.46	5704.97
Peppers.tiff	1423.18	1423.18	522.12	5699.93
Splash.tiff	1250.83	1250.83	531.86	5681.52
Tree.tiff	1490.43	1490.43	527.15	5675.60

difference between the standard deviation of the cover image and the standard deviation of the stego image is called the divergence of standard deviation. The percentage of the divergence of standard deviation helps to perform steganalysis. In the same way, the divergence of entropy is calculated.

3.4. Testing Standard Deviation

First, there needs to measure the standard deviation of the cover image to test the divergence of standard deviation. Secondly, standard deviation of the stego image needs to be observed measure. The difference between two standard deviations is called divergence of standard deviation. In addition, the divergence is calculated in percentage for each method. The strength of indemnity depends on the small divergence of standard deviation. If a method has a small divergence value, the method will show a strong security environment. In the long run, minimization of divergence standard deviation is a goal of data hiding. The divergence of standard deviation is shown in Figure 8.

The relative work focuses on achieving high image fidelity at the low payload. The proposed method's objective is to increase the payload. In Peng *et al.*'*s* scheme, the payload number is lower than the proposed scheme. Similarly, in Wang *et al.*'*s* and Weng *et al.*'*s* scheme, the payload number is lower than the proposed scheme. For this reason, the divergence of standard deviation in the proposed scheme is higher than the Peng *et al.*'*s* scheme, Wang *et al.*'*s* scheme, and Weng *et al.*'*s* scheme. In Figure 8 standard deviation of Peng *et al.*'*s*, Wang *et al.*'*s*, Weng *et al.*'*s*, and the proposed scheme are pictorially represented.

Although the relative works give a better standard deviation, the relative work does not carry a higher embedding payload. From Table 5, the values of payloads per standard deviation can be observed, and the proposed scheme presents higher values.

3.5. Testing Entropy

The divergence of the stego image and the original image is calculated from relative entropy. The relative entropy (*D*) between the probability distributions of the original image (*I*) and the stego image (*S*) is calculated by using Equation (3)-

$$D\left(I \parallel \tilde{I}\right) = \sum_{x=0}^{255} I\left(x\right) \log_{10} \frac{I\left(x\right)}{\tilde{I}\left(x\right)} \tag{3}$$

The value of relative entropy can be zero when the stego image and the cover image coincide with each other. The relative entropy becomes a small value

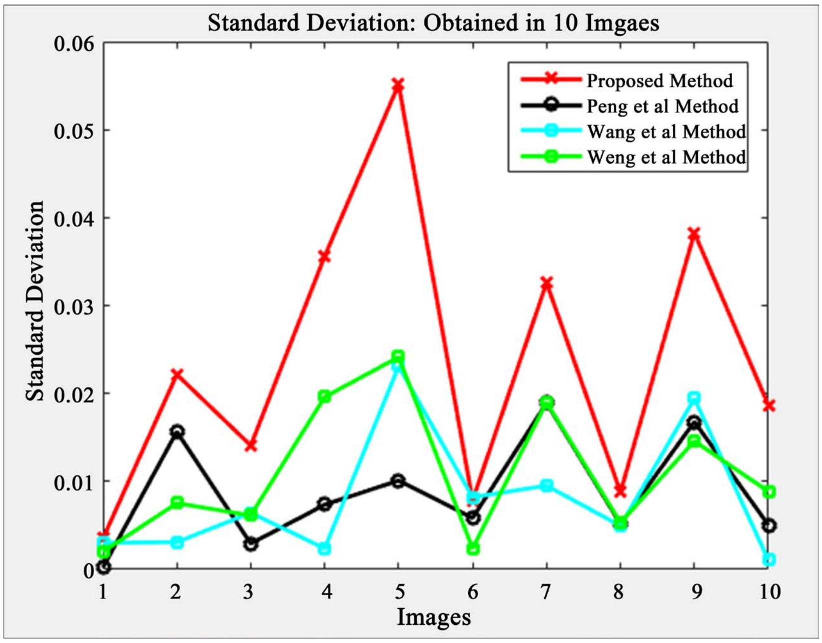

Figure 8. Comparison of standard deviation among difference schemes.

when the pixel values are very close. The higher relative value representing the pixels is not close to the stego and the cover image. In Figure 9, the entropy of different schemes is depicted.

The relative work focuses on achieving high image fidelity at the low payload. The proposed method's objective is to increase payload and minimize distortion in the image. In Peng *et al.'s* scheme, the payload number is lower than the proposed scheme. Similarly, in Wang *et al.'s* and Weng *et al.'s* scheme, the payload number is lower than the proposed scheme. For this reason, the relative entropy in the proposed scheme is higher than Peng *et al.'s* scheme, Wang *et al.'s* scheme, and Weng *et al.'s* scheme. In Figure 9 and Table 5 the relative entropy of Peng *et al.'s*, Wang *et al.'s*, Weng *et al.'s*, and the proposed schemes are pictorially represented.

Table 5. Comparison of Payloads per standard deviation with proposed one.

Images Name	In Peng *et al.*	In Wang *et al.*	In Weng *et al.*	In Proposed
Airplane.tiff	521,025,846.7	9,674,173.847	16,095,721.67	83,529,286.86
Baboon.tiff	4,495,835.114	2,007,564.686	4,285,072.027	13,209,543.22
Couple.tiff	27,266,752.92	7,846,830.647	5,247,058.079	20,783,773.76
Female1.tiff	15,943,312.5	28,530,949.43	1,645,640.828	8,221,314.234
Female2.tiff	9,471,808.212	2,077,438.804	1,336,134.712	5,309,887.541
House.tiff	15,692,580.3	5,613,813.453	13,487,847.72	37,320,850.47
Lake.tiff	3,862,020.352	1,478,769.606	1,698,085.991	8,987,448.212
Peppers.tiff	15,265,303.3	3,781,043.189	6,057,529.165	33,288,289.06
Splash.tiff	4,105,601.911	1,466,724.308	2,211,276.135	7,651,684.365
Tree.tiff	16,441,311.6	32,470,795.18	3,635,241.781	15,677,179.49

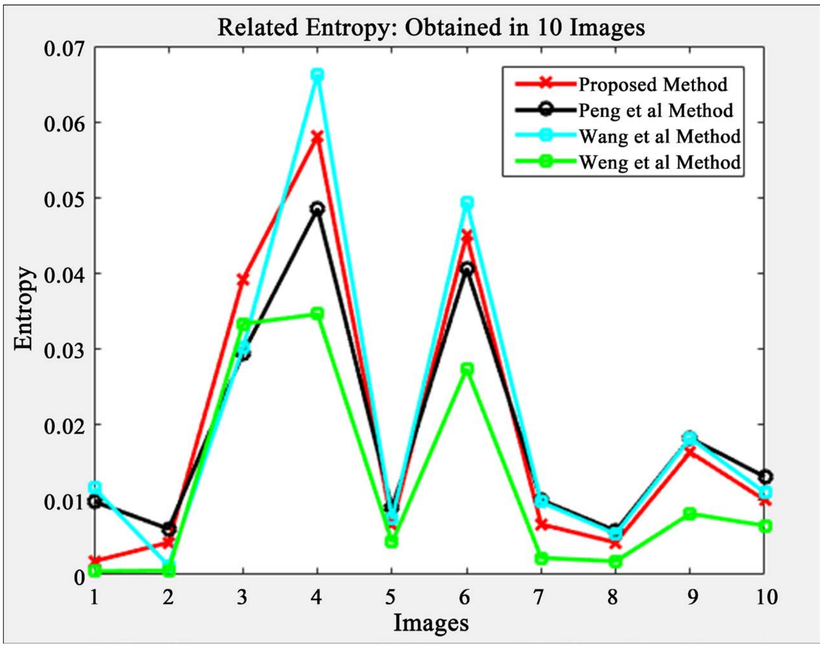

Figure 9. Comparison of entropy among different schemes.

Table 6. Comparison of payloads per entropy with proposed one.

Images Name	In Peng *et al.*	In Wang *et al.*	In Weng *et al.*	In Proposed
Airplane.tiff	11,384,707.12	64,314,574.11	70,829,248.97	165,164,588.10
Baboon.tiff	11,625,022.36	11,546,974.01	59,730,963.40	68,721,301.75
Couple.tiff	2,726,919.96	1,519,830.88	970,883.51	7,481,349.21
Female1.tiff	2,421,029.44	1,976,067.68	934,854.53	5,039,110.98
Female2.tiff	10,910,080.67	11,185,864.42	7,518,776.74	43,773,182.85
House.tiff	2,260,389.605	1,689,553.21	1,183,120.03	6,514,527.63
Lake.tiff	7,382,294.72	6,294,121.40	14,398,678.70	43,912,922.66
Peppers.tiff	13,583,734.36	10,610,285.60	18,261,035.73	68,713,476.66
Splash.tiff	3,813,608.163	3,528,032.21	3,995,340.11	18,065,487.64
Tree.tiff	6,387,583.574	5,309,676.82	4,969,810.67	29,604,351.52

Although the relative work gives better relative entropy, the relative work does not carry higher embedding bits than the proposed method. Table 6 states that the payloads per entropy are higher in the proposed scheme.

4. Conclusions

Literature suggests that the reversible schemes suffer from the lower embedding capacity. However, application areas like forensic medical, military, and law enforcement agencies must utilize both the extracted secrets and the retrieved cover image to their further processing stages. Consequently, researchers are working on increasing the embedding capacity and the stego image quality enhancement field. The proposed research used a reversible data hiding method for increasing the embedding capacity through block mean insertion and dual stego generation strategy. The scheme has experimented on a total of 499 different image datasets.

Wang *et al.*'s used a dynamic blocking strategy, although the scheme suffers from inefficiency and comprehensiveness. The proposed scheme traces the demerit and successfully applies an efficient and comprehensive approach. A good number of blocks in the competing works cannot conceive data only for the threshold mismatching. On the other hand, if a block's complexity does not match the requirement of data embedment, there will be no chance of data embedment. The proposed scheme exploits a new strategy where complexity measurement and thresholding are not required. Hence, the proposed method embeds a higher number of payloads than the competing works. Therefore, authors believe that it will be marked as a notable contribution in the research arena. Based on the experimental results, authors inferred that proposed scheme dominates the scheme of Peng *et al.'s*, Wang *et al.'s*, and Weng *et al.'s* regarding the embedding capacity by 236.72%, 750.85%, and 807.51% consecutively.

Acknowledgements

The research work is done with the support of the ICT division of the Ministry of Post, Telecommunication and Information Technology of the Government of Bangladesh through their Information and Communication Technology Fellowship program. Hence, the authors are happy to acknowledge that remarkable support.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Cox, I., Miller, M., Bloom, J., Fridrich, J. and Kalker, T. (2007) Digital Watermarking and Steganography. Morgan Kaufmann, Burlington. https://doi.org/10.1016/B978-0-12-372585-1.X5001-3

[2] Fridrich, J. (2009) Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9781139192903

[3] Ulutas, M., Ulutas, G. and Nabiyev, V.V. (2011) Medical Image Security and EPR Hiding Using Shamir's Secret Sharing Scheme. *Journal of Systems and Software*, **84**, 341-353. https://doi.org/10.1016/j.jss.2010.11.928

[4] Kamal, A.H.M. and Islam, M.M. (2014) Facilitating and Securing Offline E-Medicine Service through Image Steganography. *Healthcare Technology Letters*, **1**, 74-79. https://doi.org/10.1049/htl.2013.0026

[5] Weng, C.Y., Zhang, Y.H., Lin, L.C. and Wang, S.J. (2013) Visible Watermarking Images in high Quality of Data Hiding. *The Journal of Supercomputing*, **66**, 1033-1048. https://doi.org/10.1007/s11227-013-0969-9

[6] Xia, Z., Wang, X., Sun, X., Liu, Q. and Xiong, N. (2016) Steganalysis of LSB Matching Using Differences between Nonadjacent Pixels. *Multimedia Tools and Applications*, **75**, 1947-1962. https://doi.org/10.1007/s11042-014-2381-8

[7] Xia, Z., Wang, X., Sun, X. and Wang, B. (2014) Steganalysis of Least Significant Bit Matching Using Multi-Order Differences. *Security and Communication Networks*, **7**, 1283-1291. https://doi.org/10.1002/sec.864

[8] Chen, B.J., Shu, H.Z., Coatrieux, G., Chen, G., Sun, X.M. and Coatrieux, J.L. (2015) Color Image Analysis by Quaternion-Type Moments. *Journal of Mathematical Imaging and Vision*, **51**, 124-144. https://doi.org/10.1007/s10851-014-0511-6

[9] Liu, C.L. and Liao, S.R. (2008) High-Performance JPEG Steganography Using Complementary Embedding Strategy. *Pattern Recognition*, **41**, 2945-2955. https://doi.org/10.1016/j.patcog.2008.03.005

[10] Chao, R.M., Wu, H.C., Lee, C.C. and Chu, Y.P. (2009) A Novel Image Data Hiding Scheme with Diamond Encoding. *EURASIP Journal on Information Security*, **2009**, Article No. 658047. https://doi.org/10.1155/2009/658047

[11] Hong, W. and Chen, T.S. (2011) A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. *IEEE Transactions on Information Forensics and Security*, **7**, 176-184. https://doi.org/10.1109/TIFS.2011.2155062

[12] Böhme, R. and Kirchner, M. (2013) Counter-Forensics: Attacking Image Forensics. In: Sencar, H. and Memon, N., Eds., *Digital Image Forensics*, Springer, New York, 327-366. https://doi.org/10.1007/978-1-4614-0757-7_12

[13] Coatrieux, G., Lecornu, L., Sankur, B. and Roux, C. (2006) A Review of Image Wa-

termarking Applications in Healthcare. 2006 *International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, 30 August-3 September 2006, 4691-4694.

[14] Kamal, A.H.M. and Islam, M.M. (2017) Enhancing Embedding Capacity and Stego Image Quality by Employing Multi Predictors. *Journal of Information Security and Applications*, **32**, 59-74. https://doi.org/10.1016/j.jisa.2016.08.005

[15] Shi, Y. Q., Li, X., Zhang, X., Wu, H.T. and Ma, B. (2016) Reversible Data Hiding: Advances in the Past Two Decades. *IEEE Access*, **4**, 3210-3237. https://doi.org/10.1109/ACCESS.2016.2573308

[16] Tang, M., Hu, J. and Song, W. (2014) A High Capacity Image Steganography Using Multi-Layer Embedding. *Optik*, **125**, 3972-3976. https://doi.org/10.1016/j.ijleo.2014.01.149

[17] Zeng, X.T. and Li, Z. (2012) Reversible Data Hiding Scheme Using Reference Pixel and Multi-Layer Embedding. *AEU-International Journal of Electronics and Communications*, **66**, 532-539. https://doi.org/10.1016/j.aeue.2011.11.004

[18] Lee, C.F. and Huang, Y.L. (2012) An Efficient Image Interpolation Increasing Payload in Reversible Data Hiding. *Expert Systems with Applications*, **39**, 6712-6719. https://doi.org/10.1016/j.eswa.2011.12.019

[19] Sultana, H., Kamal, A.H.M. and Islam, M.M. (2016) Enhancing the Robustness of Visual Degradation Based HAM Reversible Data Hiding. *Journal of Computer Science*, **12**, 88-97. https://doi.org/10.3844/jcssp.2016.88.97

[20] Kamal, A.H.M. and Islam, M.M. (2018) An Image Distortion-Based Enhanced Embedding Scheme. *Iran Journal of Computer Science*, **1**, 175-186. https://doi.org/10.1007/s42044-018-0016-3

[21] Tai, W.L., Yeh, C.M. and Chang, C.C. (2009) Reversible Data Hiding Based on Histogram Modification of Pixel Differences. *IEEE Transactions on Circuits and Systems for Video Technology*, **19**, 906-910. https://doi.org/10.1109/TCSVT.2009.2017409

[22] Lee, J.D., Chiou, Y.H. and Guo, J.M. (2013) Information Hiding Based on Block Match Coding for Vector Quantization-Compressed Images. *IEEE Systems Journal*, **8**, 737-748. https://doi.org/10.1109/JSYST.2012.2232551

[23] Tang, M., Zeng, S., Chen, X., Hu, J. and Du, Y. (2016) An Adaptive Image Steganography Using AMBTC Compression and Interpolation Technique. *Optik*, **127**, 471-477. https://doi.org/10.1016/j.ijleo.2015.09.216

[24] Sajedi, H. (2016) Steganalysis Based on Steganography Pattern Discovery. *Journal of Information Security and Applications*, **30**, 3-14. https://doi.org/10.1016/j.jisa.2016.04.001

[25] Kar, D.C. and Mulkey, C.J. (2015) A Multi-Threshold Based Audio Steganography Scheme. *Journal of Information Security and Applications*, **23**, 54-67. https://doi.org/10.1016/j.jisa.2015.02.001

[26] Li, X., Zhang, W., Gui, X. and Yang, B. (2013) A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification. *IEEE Transactions on Information Forensics and Security*, **8**, 1091-1100. https://doi.org/10.1109/TIFS.2013.2261062

[27] Peng, F., Li, X. and Yang, B. (2014) Improved PVO-Based Reversible Data Hiding. *Digital Signal Processing*, **25**, 255-265. https://doi.org/10.1016/j.dsp.2013.11.002

[28] Qu, X. and Kim, H.J. (2015) Pixel-Based Pixel Value Ordering Predictor for High-Fidelity Reversible Data Hiding. *Signal Processing*, **111**, 249-260.

https://doi.org/10.1016/j.sigpro.2015.01.002

[29] Hong, W., Chen, T.S. and Chen, J. (2015) Reversible Data Hiding Using Delaunay Triangulation and Selective Embedment. *Information Sciences*, **308**, 140-154. https://doi.org/10.1016/j.ins.2014.03.030

[30] Wang, X., Ding, J. and Pei, Q. (2015) A Novel Reversible Image Data Hiding Scheme Based on Pixel Value Ordering and Dynamic Pixel Block Partition. *Information sciences*, **310**, 16-35. https://doi.org/10.1016/j.ins.2015.03.022

[31] Weng, S. and Pan, J.S. (2016) Reversible Watermarking Based on Two Embedding Schemes. *Multimedia Tools and Applications*, **75**, 7129-7157. https://doi.org/10.1007/s11042-015-2639-9

[32] Li, X., Zhang, W., Gui, X. and Yang, B. (2015) Efficient Reversible Data Hiding Based on Multiple Histograms Modification. *IEEE Transactions on Information Forensics and Security*, **10**, 2016-2027. https://doi.org/10.1109/TIFS.2015.2444354

[33] Li, X., Li, J., Li, B. and Yang, B. (2013) High-Fidelity Reversible Data Hiding Scheme Based on Pixel-Value-Ordering and Prediction-Error Expansion. *Signal Processing*, **93**, 198-205. https://doi.org/10.1016/j.sigpro.2012.07.025

[34] Weng, S., Liu, Y., Pan, J.S. and Cai, N. (2016) Reversible Data Hiding Based on Flexible Block-Partition and Adaptive Block-Modification Strategy. *Journal of Visual Communication and Image Representation*, **41**, 185-199. https://doi.org/10.1016/j.jvcir.2016.09.016

[35] He, W., Cai, J., Zhou, K. and Xiong, G. (2017) Efficient PVO-Based Reversible Data Hiding Using Multistage Blocking and Prediction Accuracy Matrix. *Journal of Visual Communication and Image Representation*, **46**, 58-69. https://doi.org/10.1016/j.jvcir.2017.03.010