Indian Journal of Science and Technology, *Vol 8(8), 731–740, April 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8i8/69310

Novel Reversible Pixel-Value-Ordering Technique for Secret Concealment

P. Subitha[1*] and V. Vaithiyanathan[2]

[1]Department of Computer Science and Engineering, SASTRA University, Thanjavur, India; subithaprithvi@gmail.com
[2]School of Computing, SASTRA University, Thanjavur, India; vvn@it.sastra.edu

Abstract

This work is to preserve the distortion of marked image from the original image, that is, to improve the Peak Signal-to-Noise Ratio (PSNR) and to improve the Embedding Capacity (EC). Pixel-Value-Ordering (PVO) is the technique used for ensuring reversibility in Reversible Data Hiding (RDH). The difference-value is calculated from ordered pixel blocks. From the difference-value histogram, the rough bins are shifted to vacate place for concealing secret whereas the smooth bins are expanded to conceal secret. The proposed Novel Reversible Pixel-Value-Ordering Technique (RPVOT) is the containment of two schemes: Novel Difference Computation (DC) and Novel Histogram Shifting (HS). Firstly, for DC, the existing approaches compute the difference between first two (or, last two) pixel values of an ordered block whereas, the novel DC technique picks up the first two pixel values (or, last two pixel values) from an ordered block and the rounded mean of pixel values in minimum and maximum position subtracted from a pixel value in minimum position is computed. This novel DC makes eligible more number of blocks for secret concealment than other existing approaches by which more secret bits can be concealed and visual worth of the marked image is conserved as well. Secondly, novel HS is proposed which break the rule of shifting all the blocks that are not meant for embedding by shifting some blocks using naturally occurring empty bins in the histogram. This novel HS prevents many blocks from unnecessary alteration in their pixel values and hence, visual worth of the marked image is improved further. Both novel DC and novel HS are combined together to form novel RPVOT which significantly improves the Embedding Capacity (EC) along with Peak Signal-to-Noise Ratio (PSNR).

Keywords: Difference Computation, Difference-Histogram, Histogram Shifting, Reversible Data Hiding, Pixel-Value-Ordering

1. Introduction

Steganography is an old art of hiding information inside another innocent medium. Since privacy is needed in every field, Steganography has been retaining its popularity in the upcoming digital world with new avatar Digital Steganography[3]. Digital Steganography deals with covert communication using digital medium. In addition to Text Steganography, Image Steganography, Audio Steganography[20] and Video Steganography[18,19], Network Steganography is the young sibling ruling the Steganography world now.

Data Embedding can be possible in both Spatial and Transform domains. Spatial domain embedding picks up the innocent host or cover medium and embeds the secret in the original pixel value itself whereas Transform domain embedding embeds the secret in the transformed pixels. Put in detail, the original spatial domain pixels are either transformed into Frequency domain or transformed into Wavelet domain and hidden is the secret data in the transformed pixels using any one the techniques avail in the transform domain. Mushrooms of techniques avail in both spatial and transform domain for covering secret. Difference Expansion (DE)[1,14], Prediction-Error Expansion (PEE)[4,7,13,17], Histogram shifting (HS)[6,9,15], Spread Spectrum (SS) are the techniques, to name a few, in spatial domain.

**Author for correspondence*

Rather than Steganography, Data Hiding is a crisp term for covert communication. In normal data hiding approaches, secret data only is the hero and cover medium is just the medium to embed. In other words, during data extraction, we bother only about secret data and not about cover medium. But in the case of Reversible Data Hiding (RDH), both the secret data and cover medium are bothered and the need is to extract both without distortion[2]. RDH has its footprint in the field of Medical, Military, etc., wherein releasing of secret from the marked-image and restoration of original image after secret extraction are of main interest.

In Tian et al.'s method[14], spatial domain technique for reversible secret hiding using DE is proposed. In DE, the pixel pair is taken into account and the difference between pixel pairs is expanded to hide secret. Alattar et al[1] improvised Tian's method[14] by utilizing spatial triplets and spatial quads instead of spatial pairs. Thodi and Rodriguez[13] have improved DE with PEE technique. PEE is expanded to hide secret and improvement in EC is achieved over DE. Hu et al[5] focused on Location Map (LM) compression and betterment in EC is realized. Adaptive embedding is carried out by segregating image into flat and rough regions in Li et al.'s art[8] which succeeded traditional PEE.

In Ni et al.'s art[9], popular Histogram-Shifting (HS) method is introduced in which the peak point and zero point in the histogram are taken and histogram bins between both points are shifted to realize embedding at the peak point. This art ensures reversibility and targets PSNR of atleast 48 dB. Lee et al[12] proposed a scheme with pixel pairs rather than pixel blocks which embed more bits with lesser distortion than art[9]. The difference between second pixel value and first pixel value is taken in each pixel pair and the Bins -1 and 1 are exploited to conceal secret data. In art[7], common HS framework is well explained by Li et al.

Sorting technique plays a vital role in RDH. Kamstra et al[6] sort the pixel pairs to encourage compression and thus have a small LM which produces better capacity with acceptable distortion than art[14]. Sachnev et al[15] get benefited from the sorted Prediction-Error and reduced LM and so it exceeds the arts[6,12,13] in EC.

Some recent arts that focus on better visual worth of the image include Li et al.'s[16] RDH scheme. In art[16], PVO technique is used which exploits smoother regions to embed secret. The pixel blocks are ordered and the difference between the largest and the second largest pixel value of each sorted block is taken. The blocks having pixel value difference as one, that is, Bin 1 is exploited in the histogram lying between [0, +∞] to conceal secret using maximum modification strategy. The problem in this art is that Li et al. leave the Bin 0 untouched even though Bin 0 carries smoother blocks. Recent art by Ou et al[10] improves Li et al.'s art[16] by utilizing all the minimum and maximum pixel values in a pixel block for secret embedding. By this, image redundancy is exploited and achieved is the more EC and PSNR when contrasted with art[16].

Peng et al[11] has extended the work of arts[16,12] with the newly proposed difference calculation to provide betterment in EC. It is given in art[11] that no improvement has come with while contrasting both Li et al.'s and Lee et al.'s art. The reason behind this is, Bin 1 of Li et al. is exactly same as that of sum of Bins –1 and 1 in Lee et al.'s art. Lee et al.'s extended art well introduced in art[11] exploits the image redundancy as because the two histogram bins namely Bin 0 and 1 are utilized to conceal the secret as opposed to a two Bin usage -1 and 1 in art[12]. Put more simply, the pixel pairs having difference values zero and one are used to hide secret using Lee et al.'s extended scheme and by this 16% improvement in EC is realized over Li et al.'s scheme.

Even though many prior related arts available, Peng et al.'s art[11] achieved improvement over other arts and is goodly briefed in Section 2. The modifications are made and the new novel scheme on RDH is detailed in Section 3. Performance measures such as EC and PSNR are analyzed based on the experiment on many standard images which is given in Section 4. At last, the paper is ended with conclusion part in Section 5.

2. Related Works

There is handful of related works available while considering reversible data hiding techniques with its base on PVO. Amid them, RDH scheme based on Improved PVO proposed by Peng et al. is recently proposed and is explained in Section 2.1.

2.1 Peng et al.'s PVO based RDH

Peng et al.'s work includes RDH based on Improved PVO. The PVO technique is used to achieve the reversibility property, meaning that, the original host image is extracted successfully during data extraction procedure without causing any distortion to the image.

Maximum Modification Scheme is used to hide secret in the largest or maximum or last pixel value of each block. Similarly, Minimum Modification Strategy can also be used in which the secret is hidden in the minimum or smallest pixel value, that is, the very first value of each block. By combining both Maximum and Minimum Modification Strategies, it is possible to hide two bits per block, one in the minimum or smallest pixel value and the other secret bit in the maximum or largest pixel value. For better understanding, Maximum Modification Strategy is explained briefly in Section 2.1.1.

2.1.1 Maximum Modification Scheme

Step-1 Chop the original host image into several, equal, non-overlapping blocks. Let $x_1, x_2, \ldots, x_n$ be the pixel values in a pixel block and $posx_1, posx_2, \ldots, posx_n$ be the corresponding positions.

Step-2 Pixels in each block is sorted in ascending order. Let the sorted pixel values in each block be $x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}$. $x_{\sigma(1)}$ denotes the smallest or minimum pixel value and $x_{\sigma(n)}$ denotes the largest or maximum pixel value.

Step-3 The position of pixel values before and after sorting may get changed. Let the position after sorting be $posx_{\sigma(1)}, posx_{\sigma(2)}, \ldots, posx_{\sigma(n)}$. Now the position of the largest or maximum pixel value, $posx_{\sigma(n)}$ is compared with the position of the second largest pixel value, $posx_{\sigma(n-1)}$.

$$\begin{cases} u = min(posx_{\sigma(n)}, posx_{\sigma(n-1)}) \\ v = max(posx_{\sigma(n)}, posx_{\sigma(n-1)}) \end{cases} \quad (1)$$

Step-4 The difference value is calculated as follows:

$$d_{max} = x_u - x_v \quad (2)$$

Step-5 The difference value, d_{max} of each block is taken to plot the histogram. d_{max} with 0 and 1 are used to hide the secret, that is, histogram bins 0 and 1 are expanded for embedding secret. Simply put, the blocks having difference values 0 and 1 are taken in which the largest pixel value is utilized for embed the secret. The histogram modification procedure of Peng et al. is depicted in Figure 1.

$$\bar{d}_{max} = \begin{cases} d_{max} - 1, & \text{if } d_{max} < 0 \\ d_{max} - b, & \text{if } d_{max} = 0 \\ d_{max} + b, & \text{if } d_{max} = 1 \\ d_{max} + 1, & \text{if } d_{max} > 1 \end{cases} \quad (3)$$

Step-6 The last or largest pixel, x_{max} in each block is modified to:

$$\bar{x}_{max} = \begin{cases} x_{max} - 1, & \text{if } d_{max} < 0 \\ x_{max} - b, & \text{if } d_{max} = 0 \\ x_{max} + b, & \text{if } d_{max} = 1 \\ x_{max} + 1, & \text{if } d_{max} > 1 \end{cases} \quad (4)$$

As the largest pixel value after embedding secret is either unaltered or incremented by 1, the sorting order does not change. By this, the concealed bits are extracted and the original host image can be restored without any distortion after performing data extraction. Minimum Modification Scheme of Peng et al. follows the same procedure as above, but with the simple change of performing the difference computation using the first two pixel values of a block.

2.1.2 Data Extraction

Upon extraction, the secret is unlocked from the marked image and the real host image is to be recovered without any distortion.

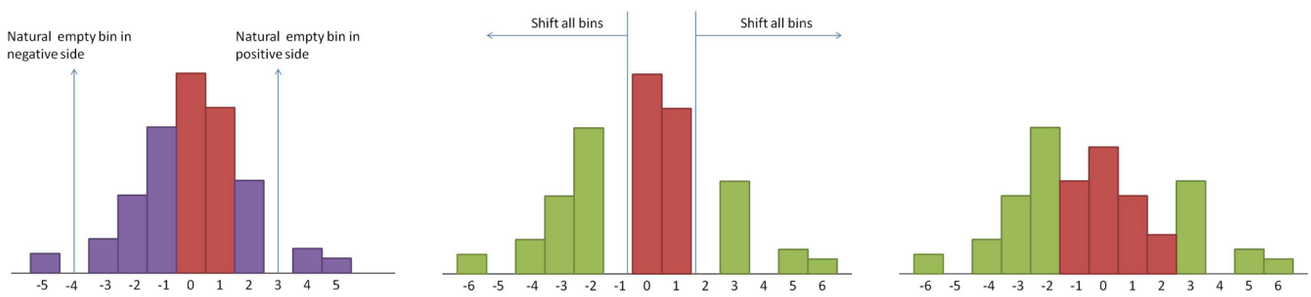

Figure 1. Peng et al.'s Histogram Modification Scheme. a) Original Difference-Histogram. b) Bin Shifting Procedure. c) After Secret Concealment.

- **Secret Bit Extraction:** The secret bit is released from the marked image as follows:

$$b = \begin{cases} 1, & \text{if } \bar{d}_{max} = -1, 2 \\ 0, & \text{if } \bar{d}_{max} = 0, 1 \end{cases} \quad (5)$$

There is no secret bit hidden in the block, if the block contains difference value, $\bar{d}_{max}$ lesser than –1 or difference value, $\bar{d}_{max}$ greater than 2.

- **Original Image Restoration:** The original host image is restored by predicting the largest or last pixel value of an eligible block. The maximum or largest pixel in each block is predicted using difference value, $\bar{d}_{max}$ as follows:

$$x_{max} = \begin{cases} \bar{x}_{max} + 1, & \text{if } \bar{d}_{max} < -1 \\ \bar{x}_{max} + b, & \text{if } \bar{d}_{max} = -1, 0 \\ \bar{x}_{max} - b, & \text{if } \bar{d}_{max} = 1, 2 \\ \bar{x}_{max} - 1, & \text{if } \bar{d}_{max} > 2 \end{cases} \quad (6)$$

By this procedure, reversibility is achieved. Using PVO, the first and last altered pixel values of eligible blocks are predicted and are contracted to get the concealed secret bits if blocks lies in the bins –1,0,1 and 2. The blocks are shifted back to the original bin locations if the difference value is lesser than –1 or greater than 2 to restore the image back. This paves the way for releasing the secret bits out and the marked image is restored to the original image as such without any distortion.

3. Proposed System

The novel scheme of DC and HS is proposed in this section. Taking into account the last two pixel values of each sorted block in the case of Maximum Modification Scheme and the first two pixel values of each sorted block in the case of Minimum Modification Scheme, the novel difference calculation is carried out by taking difference of rounded mean of pixel values in minimum and maximum position from pixel value in the minimum position. Making use of the empty bins which occur naturally in the difference histogram, the novel HS strategy is introduced that prevents some sorted block's last (or, first) pixel value from being changed by allowing only the bins upto the first empty bin to get shifted.

3.1 Novel Difference Computation

The host image is chopped into several equal non-overlapping blocks and pixel values in each block are sorted in ascending order along with position. This novel difference computation applies to both Maximum and Minimum modification strategy. The Maximum Modification Scheme picks up the last two pixel values whereas the Minimum Modification Scheme consider the first two pixel values of sorted block for performing difference computation. Let $x_1, x_2, \ldots, x_n$ be the pixel values, $x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}$ be the sorted pixel values and $posx_{\sigma(1)}, posx_{\sigma(2)}, \ldots, posx_{\sigma(n)}$ be the position of pixel values after sorting alike the Peng et al.'s art.

In Maximum modification scheme, the very last pixel value of sorted block is either increased by 1 or unaltered during secret concealment. The block whether is eligible for hiding or not is decided by the difference value. The last two pixel values are taken into account from a sorted block and the sorted positions of both pixel values are compared. The rounded mean of two taken pixel values is subtracted from the pixel value in the minimum position 'u' to get the difference value.

$$diff_{max} = x_u - v \quad (7)$$

where

$$\begin{cases} u = min(posx_{\sigma(n)}, posx_{\sigma(n-1)}) \\ v = round(\frac{x_{\sigma(n)} + x_{\sigma(n-1)}}{2}) \end{cases} \quad (8)$$

In Minimum modification Scheme, the very first pixel value of sorted block is either decreased by 1 or unaltered to hold secret bit. Here too, the difference value decides whether to shift or expand or do nothing with the block. For computing the difference value, pixel values in first two sorted positions are picked up. Alike maximum modification strategy, the rounded mean of two taken pixel values is subtracted from the pixel value in the minimum position to obtain the difference value.

$$diff_{min} = x_u - v \quad (9)$$

where

$$\begin{cases} u = min(posx_{\sigma(1)}, posx_{\sigma(2)}) \\ v = round(\frac{x_{\sigma(1)} + x_{\sigma(2)}}{2}) \end{cases} \quad (10)$$

By this novel difference computation, chosen are the more number of blocks for concealing secret. Also,

for lesser threshold, concealed are the more secret bits when compared with the number of bits concealed by Peng et al[11].

3.2 Novel Histogram Shifting

The difference histograms are plotted using $diff_{min}$ and $diff_{max}$ of all sorted blocks. The difference value $diff_{min}$ is for hiding secret at the very first pixel value and the difference value $diff_{max}$ is for concealing secret at the very last pixel value of an eligible block. Histogram modification involves two things: Shifting and Expansion. Rough blocks are shifted for vacating place for carrying secret data and Smooth blocks are expanded to hold the secret data. Histogram having bins 0 and 1 are used for concealing secret data as because those bins are the residence for smoother blocks. For doing so, bins -1 and 2 are emptied out by shifting all bins other than bins 0 and 1. Put in detail, *Bins* < 0 are shifted one time left and *Bins* > 1 are shifted one time right which has its effect of emptying out bins –1 and 2 and then bins 0 and 1 are expanded to lock the secret bits. Histogram bins –1,0,1,2 hold the secret data after data embedding.

In motive of improving PSNR, novel HS is introduced, wherein naturally occurring empty bins are sought while shifting bins that are not meant for embedding. The bins upto the first empty bin are shifted on both sides leaving the other bins untouched. This scheme prevents many pixel values from changes and thus visual quality of the image is highly preserved. The novel histogram modification is explained in Figure 2.

3.2.1 *Maximum and Minimum Modification Strategy*

In maximum modification strategy, the smooth bins 0 and 1 are expanded to conceal secret. Some blocks which are not lying in the bins 0 and 1 are shifted. Blocks in the bins that are greater than 1 and are lesser than first empty bin of positive side are shifted one time right. Blocks that are lesser than 0 and are greater than first empty bin of negative side are shifted one time left. So, the difference value $diff_{max}$ is modified to:

$$\overline{diff}_{max} = \begin{cases} diff_{max} - 1, & \text{if } empty^{-} < diff_{max} < 0 \\ diff_{max} - b, & \text{if } diff_{max} = 0 \\ diff_{max} + b, & \text{if } diff_{max} = 1 \\ diff_{max} + 1, & \text{if } 1 < diff_{max} < empty^{+} \end{cases} \quad (11)$$

The last or maximum element of an eligible block is modified to:

$$\bar{x}_{max} = \begin{cases} x_{max} - 1, & \text{if } empty^{-} < diff_{max} < 0 \\ x_{max} - b, & \text{if } diff_{max} = 0 \\ x_{max} + b, & \text{if } diff_{max} = 1 \\ x_{max} + 1, & \text{if } 1 < diff_{max} < empty^{+} \end{cases} \quad (12)$$

The data embedding and the HS procedure for the Minimum Modification Strategy are same as that of Maximum modification strategy. So, the difference value $diff_{min}$ is modified to:

$$\overline{diff}_{min} = \begin{cases} diff_{min} - 1, & \text{if } empty^{-} < diff_{min} < 0 \\ diff_{min} - b, & \text{if } diff_{min} = 0 \\ diff_{min} + b, & \text{if } diff_{min} = 1 \\ diff_{min} + 1, & \text{if } 1 < diff_{min} < empty^{+} \end{cases} \quad (13)$$

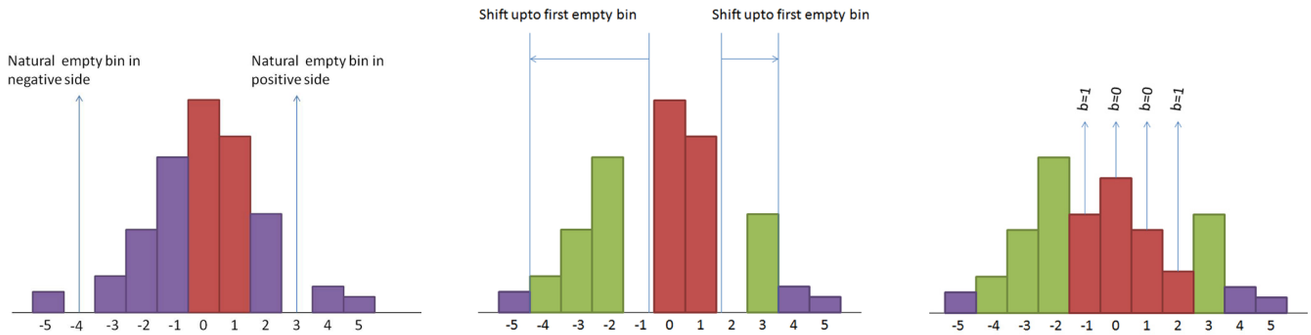

Figure 2. Proposed Novel Histogram Modification Scheme. a) Original Difference-Histogram. b) Bin Shifting Procedure. c) After Secret Concealment. 'b' indicate the concealed secret bit.

The first element of each sorted block is modified to:

$$\bar{x}_1 = \begin{cases} x_1 - 1, & \text{if } empty^- < diff_{min} < 0 \\ x_1 - b, & \text{if } diff_{min} = 0 \\ x_1 + b, & \text{if } diff_{min} = 1 \\ x_1 + 1, & \text{if } 1 < diff_{min} < empty^+ \end{cases} \quad (14)$$

The notation $empty^-$ refers to first negative empty bin in the difference histogram and the notation $empty^+$ refer the first empty bin of positive side of difference histogram. Empty bins are naturally occurring, meaning that, count of blocks having that particular difference value is zero. Put in other words, there is no block having that particular difference value. For instance, if empty bin lies in difference value 4, it means that no blocks do have the difference value 4 and hence, #diff=0 for the difference value 4. Only the first empty bins on both sides are considered here. These empty bin values are in need at the extractor side to shift the histogram back to its normal bin positions.

Novel RPVOT follows the same Data extraction procedure as that of art[11]. The secret extraction and Image restoration are done using equations in Section (2.1.2) with a simple variation. The data extraction procedure follows the equation:

$$x_{max} = \begin{cases} \bar{x}_{max} + 1, & \text{if } empty^- \le \bar{d}_{max} < -1 \\ \bar{x}_{max} + b, & \text{if } \bar{d}_{max} = -1, 0 \\ \bar{x}_{max} - b, & \text{if } \bar{d}_{max} = 1, 2 \\ \bar{x}_{max} - 1, & \text{if } 2 > \bar{d}_{max} \ge empty^+ \end{cases} \quad (15)$$

In this way, the secret bits are unlocked and the image is restored back at the extractor side. The same extraction procedure is imitated for the Minimum Modification Strategy.

3.3 Block Selection Criteria

The secret is concealed in the blocks which passes the block eligibility criteria. The basic aim is to conceal by exploiting the smoother blocks. For selecting the smooth blocks, Noise Level (NL) for each block should be computed. Leaving the first and last pixel values, the difference between the remaining pixel values are taken as the NL value. This value does not change even after secret concealment. The reason is that, after concealing secret, only the very first and very last pixel value do undergo change. The big thing is, we need not send NL value to the other end and is computed at the extraction side itself. The NL is computed as follows:

$$NL = x_{\sigma(n-1)} - x_{\sigma(2)} \quad (16)$$

It is also mandatory to check the Location Map (LM) which ensures whether overflow or underflow occur in the blocks or not. Overflow occurs when the pixel value 255 is attempted to change to 256 which is out of bound for the gray-scale images whose pixel values normally lies between 0 and 255. Underflow occurs when the pixel value 0 is viable to become -1. To avoid this to happen, the blocks having pixel value 0 or 255 are marked as 1 and the remaining blocks are marked to 0. The secret can be concealed only if the block fulfills the block selection criteria based on NL and LM value. The LM value is marked as follows:

$$LM = \begin{cases} 0, \ if \ not, \ 0 \ and \ 255 \\ 1, \ if, \ 0 \ or \ 255 \end{cases} \quad (17)$$

- If $NL < Threshold$ and $LM = 0$, block is eligible for concealing secret.
- If $NL > Threshold$ or $LM = 1$, block obviously cannot hold secret.

Initially, Threshold value is set to 1 and is gradually incremented by 1 until the fixed number of secret bits can be locked into the image. As the Threshold value increases, the eligible blocks also increases which paves the way for embedding more secret bits but showering bad effect in the visual quality of the image. Simply put, as Threshold increases, EC also increases with reduction in PSNR.

3.4 Secret Concealment

Explained here are the detailed steps involved in the Embedding and Extraction procedure of proposed Novel RPVOT.

3.4.1 Embedding Procedure

Step-1 (Chop and Sort): The original gray-scale image of size 512 x 512 is chopped into several non-overlapping blocks of varying sizes chosen from the 16 possible combination of {2,3,4,5} and the one that produces better PSNR is taken into account. Each block along with the position is sorted in ascending order.

Step-2 (Build NL and LM): For each block, NL and LM are calculated using Equations (16) and (17) respectively.

As NL is unchanged even after secret hiding, there is not any need to send NL as an extra information. But LM is viable to change as because 0 and 255 are possible pixel values after secret embedding and so is compressed using arithmetic coding and the need is to send Compressed Location Map (CLM) and length of CLM (l_{CLM}) as an extra stuff.

Step-3 (Split-Up and Lock Secret in Organ 'A'): The Host Image is split-up into two Organs: say A and B. If the block selection criteria satisfies, that is, if $NL < Threshold$ and $LM = 0$, then secret bits are hidden in the eligible blocks using Maximum and Minimum modification strategy in Organ 'A'. At the maximum, two bits can be locked per block. The block where the secret bit ends is the end of Organ 'A' and the block next to it is the start of Organ 'B'. End of Organ 'A' is marked as P_{end} and is one of the key to be embedded for unlocking secret. The image now obtained is the partially concealed image which is fed up to the next stage.

Step-4 (Make SLSB and Lock SLSB in Organ 'B'): Extra key information for unlocking the secret is needed at the extractor side and hence is locked in the LSBs of first several pixels of partially concealed image. The issue is to restore the host image as such and so, just replacing the LSBs by key information is not an good idea. The original LSBs of first several pixels are first stored as binary sequence, say SLSB and then LSBs can be replaced with the key information. Organ 'B' is the residence for SLSB and hence, if the block selection criteria satisfies, that is, if $NL < Threshold$ and $LM = 0$, SLSB is hidden in the eligible blocks using Maximum and Minimum modification strategy in Organ 'B'. At the maximum, two bits can be locked per block.

Step-5 (Replace LSBs with Key information): The vacated LSBs of first several pixels are replaced with the extra key information that holds the information needed for releasing secret from the organs. The key includes the following:

- **Block size**- $n_1, n_2 \in [2, 3, 4, 5]$. 3 bits for each n_1 and n_2 is required. It consumes 6 bits in total for indicating block size and the first 6 pixel value's LSBs are replaced with block size.
- **NL Threshold**- 8 bits are needed. Replaced are the LSBs of pixel values from 7 to 14 for hiding key, NL Threshold.
- **Empty$^-$ and Empty$^+$**- Both takes values from 0 to 255 and so 8 bits are needed to represent each. As two histograms are plotted, one for the difference values, d_{max} and other for the difference values, $d_{min,}$ two empty$^-$ and two empty$^+$ values exist. In total (8 x (2+2) = 32 bits are required).
- **End of Organ 'A'**- P_{end} value needs $[log_2 N]$ bits.
- l_{CLM}- Length of CLM requires $[log_2 N]$ bits.
- **CLM**- Compressed Location Map needs l_{CLM} bits.

Firstly, first $46 + 2[log_2 N] + l_{CLM}$ number of pixel values are exploited and their LSBs are stored as SLSB and then those LSBs are replaced with extra key information specified above.

3.4.2 Extraction Procedure

Step-1 (Release Key Information): The first $46 + 2[log_2 N] + l_{CLM}$ LSBs are exploited to obtain the key information such as block size, threshold, P_{end}, l_{CLM} and CLM. CLM is decompressed to get LM values.

Step-2 (Unlock SLSB and Restore LSBs): By using P_{end} value, the marked image is split-up into two Organs 'A' and 'B'. From the Organ 'B', SLSB is extracted using extraction rules of Novel Maximum and Minimum modification strategy. The extracted binary sequence is then replaced with LSBs of first $46 + 2[log_2 N] + l_{CLM}$ pixel values to restore the original LSBs.

Step-3 (Unlock Secret and Restore Host Image): Now, the turn is to unlock the secret bits from Organ 'A'. The same extraction procedure of Novel maximum and minimum modification strategy is applicable for doing this secret extraction and Host Image restoration.

4. Experimental Results

Experiments are conducted on various 512 x 512 sized standard gray-scale images taken from the standard database. The images including Lena, Baboon, Airplane, Peppers, Sailboat, Fishing boat, Elaine and Tiffany are taken from the standard USC-SIPI Image Database[21]. Images Lena, Baboon, Airplane, Peppers, Sailboat and Tiffany are 512 x 512 24-bit images which are first converted to 8-bit images and then performance is analyzed. Fishing boat and Tiffany images are 512 x 512 sized standard gray-scale images and so they are used directly. Barbara image is taken from the standard dataset of 512 x 512 gray-scale images[22]. Some of the sample gray-scale converted test images are shown in Figure 3.

Figure 3. Sample Images from the Standard Database. a) Lena. b) Baboon. c) Airplane. d) Peppers. e) Sailboat. f) Elaine. g) Barbara.

When our proposed RPVOT is contrasted with arts[11,16], maximum bits to be embedded is improved along with improvement in PSNR. The high EC is proved through the lesser NL threshold value. The novel difference computation makes possible the more number of blocks eligible for embedding. This restricts the threshold value to somewhat a smaller value when compared with art[11]. Lesser Threshold indirectly means that more blocks are eligible which in turn ensures more is the EC. One more thing to note is that, if more blocks can hold secret, by fixing the EC to some bits, PSNR will also be increased to a good rate when contrasted with the existing arts. The contrast between our proposed RPVOT and previous art[11] in terms of EC Vs Threshold for some test images are graphically depicted in Figure 4.

From Figure 4, it is clear that very less threshold value is enough to select suffice blocks for holding fixed secret bits. Also when EC reaches high, tremendous reduction in threshold is seen. The best block size is chosen for each image from the best PSNR achieved among the 16 possible block size combinations. The best block size for each image and its threshold value for embedding a fixed EC of about 10000 bits is given in Table 1.

The graphical picture of comparison of Proposed work against Peng et al.'s work for various standard images like Lena, Baboon, Airplane, Peppers, etc., are shown in Figure 5. With a gradual increment in EC of 1000 bits, PSNR is plotted for varying Embedding rate. It is obvious that PSNR is significantly improved no matter how bad the EC is varying. Specifically, when EC is high, PSNR also stands good than the existing art. The trade-off between EC and PSNR is superbly handled by the novel RPVO technique. It is seen that, for the rough image like Baboon, the performance is even more good.

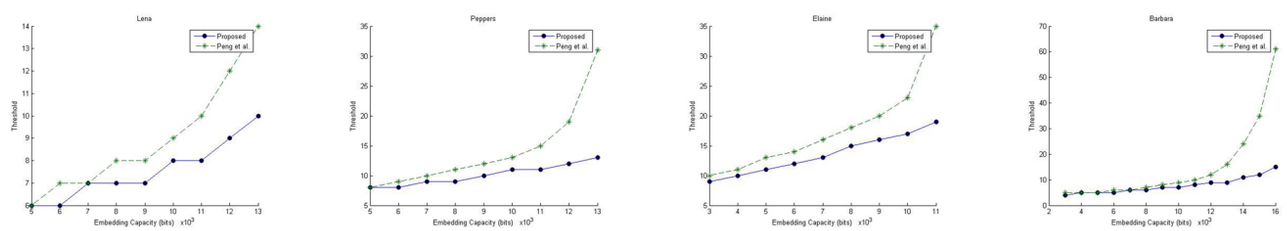

Figure 4. Contrast between Thresholds for Proposed RPVOT and Peng et al[11] by varying EC a) Lena. b) Peppers. c) Elaine. d) Barbara.

Table 1. Best Block Size and NL Threshold for Proposed RPVOT with 10000 bits fixed as an EC

Test Image	Block Size	Threshold
Lena	(4,3)	8
Baboon	(3,2)	17
Airplane	(5,2)	4
Peppers	(3,4)	11
Fishing Boat	(2,5)	12
Sailboat	(2,4)	8
Elaine	(4,3)	17
Barbara	(3,3)	7

Achievement of about 3 dB increment in PSNR is achieved over Li et al.'s art for Baboon which makes sure that image redundancy is well exploited and this novel art work well for rough images. PSNR contrast is depicted in Table 2 for the proposed art and other arts[11,16] by experimenting on the standard test images with an EC fixed as 10000 bits.

Additionally, novel HS avoids the need to shift all the bins and thus prevents some rough blocks from unnecessary changes in the last and first pixel values by utilizing naturally occurring empty bins in the difference-histogram which causes slight reduction in Mean Square Error (MSE) and the PSNR improvement is obtained which is a very slight improvement. The reason for this slight improvement is that, only lesser blocks are prevented from shifting. Also, this novel HS causes an additional 32 bits to be embedded as a key for specifying empty bin values which is mandatory to shift shifted bins back. But it is neglible because novel HS results in slight reduction of MSE.

While combining both Novel DC and Novel HS, great improvement in PSNR is achieved along with increment in EC. Our work goodly excels in PSNR lifting and it hits recent arts including Peng et al.'s art[11] , Li et al.'s art[16] and the very recently proposed art of Ou et al[10].

5. Conclusion

This work well exploits the image redundancy for concealing secret. Proposed is the Novel RPVO technique which is the containment of novel difference

Table 2. PSNR Comparison of Proposed RPVOT against Peng et al[11] and Li et al[16] with 10000 bits fixed as an EC

Test Image	Proposed	[11]	[16]
Lena	61.55	60.47	59.86
Baboon	56.70	53.55	53.50
Airplane	63.41	62.96	61.61
Peppers	60.30	58.98	58.55
Fishing Boat	59.84	58.27	57.85
Sailboat	60.33	58.87	58.18
Elaine	59.13	57.36	56.84
Barbara	61.49	60.54	59.98
Average	60.52	59.29	58.87

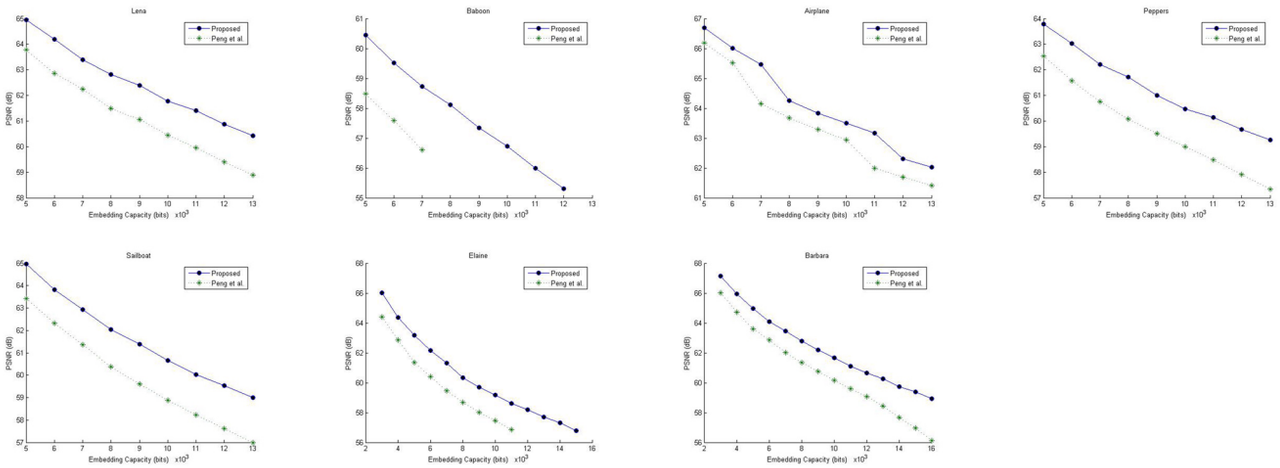

Figure 5. EC Vs PSNR of arts Peng et al[11] and Proposed RPVOT for standard images like a) Lena. b) Baboon. c) Airplane. d) Peppers. e) Sailboat. f) Elaine. g) Barbara.

computation and novel histogram shifting strategy. This proposed novelty art relaxes the block selection criteria by picking more eligible blocks for secret concealment which is ensured by the lesser NL threshold obtained and hence more is the achieved EC with significant improvement in PSNR. The credit of making more blocks eligible solely goes to the novel difference computation which brought up the PSNR by greater than 1 dB in an average and ascends the EC as well. This shows that the proposed novel RPVOT excels than the other prior works even for the rough images. Also, with the high EC and high PSNR obtained, it is obvious that, more the bits can be concealed and better is the visual worth of the marked stego-image.

6. References

1. Alattar AM. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing. 2004; 13(8):1147–56.
2. Caldelli R, Filippini F, Becarelli R. Reversible watermarking techniques: An overview and a classification. EURASIP Journal on Information Security. 2010; 2010:134546. doi:10.1155/2010/134546.
3. Artz D. Digital steganography: hiding data within data. IEEE on Internet of Computing; 2001. p. 75–80.
4. Hu Y, Lee, Heung-Kyu, Li J. DE-based reversible data hiding with improved overflow location map. IEEE Transactions on Circuits and Systems for Video Technology. 2009; 19(2):250–60.
5. Wu H-T, Huang J. Reversible image watermarking on prediction errors by efficient histogram modification. Signal Process. 2012; 92(12):3000–9.
6. Kamstra L, Heijmans HJAM. Reversible data embedding into images using wavelet techniques and sorting. IEEE Transactions on Image Processing. 2005; 14(12):2082–90.
7. Li X, Li B, Yang B, Zeng T. General framework to histogram-shifting-based reversible data hiding. IEEE Transactions on Image Processing. 2013; 23(6):2181–91.
8. Li X, Yang B, Zeng T. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. IEEE Transactions on Image Processing. 2011; 20(12):3524–33.
9. Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Transaction on Circuits System Video Technology. 2006; 16(3):354–62.
10. Ou B, Li X, Zhao Y, Ni R. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion. Image Communication, 2014; 29(7):760–72.
11. Peng F, Li X, Yang B. Improved PVO-based reversible data hiding. Digit Signal Process. 2014; 25:255–65.
12. Lee SK, Suh YH, Ho YS. (2006) Reversible image authentication based on water-marking. Proceedings of the IEEE ICME; 2006. p. 1321–4.
13. Thodi DM, Rodriguez JJ. Prediction-Error based reversiblewatermarking.ProceedingsofInternationalConferenceon Image Processing (ICIP '04). 2004; 3:1549–52.
14. Tian J. Reversible data embedding using a difference expansion. IEEE Transaction on Circuits System Video Technology. 2003; 13(8):890–6.
15. Sachnev V, Kim HJ, Nam J, Suresh S, Shi YQ. Reversible watermarking algorithm using sorting and prediction. IEEE Transactions on Circuits and Systems for Video Technology. 2009; 19(7):989–99.
16. Li X, Li J, Li B, Yang B. High-fidelity reversible data hiding scheme based on pixel value ordering and prediction error expansion. J Signal Process. 2013; 93(1):198–205.
17. Swain G. Digital image steganography using nine-pixel differencing and modified LSB substitution. Indian Journal of Science and Technology. 2014 Sep; 7(9):1444–50.
18. Ramalingam M, Isa NAM. A steganography approach over video images to improve security. Indian Journal of Science and Technology. 2015 Jan; 8(1):79–86.
19. Ramalingam M, Isa NAM. Video steganography based on integer haar wavelet transforms for secured data transfer. Indian Journal of Science and Technology. 2014 Jul; 7(7):897–904.
20. Valarmathi R, Nawaz GMK. Secure data transfer through audio signal with LSA. Indian Journal of Science and Technology. 2015 Jan; 8(1):17–22.
21. Available from: http://sipi.usc.edu/database/.
22. Available from: http://decsai.ugr.es/cvg/CG/base.htm.