I J C T A, 9(25), 2016, pp. 337-345 ISSN: 0974-5572

Enhanced Image Steganography Scheme through Multiway PVD

B. Ida Seraphim[1], **B. Sowmiya**[2] **and J. Anitha**[3]

ABSTRACT

The Pixel Value Differencing (PVD) based approach is the steganographic algorithm in spatial domain. In the process of embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human vision's sensitivity (HVS). The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The larger the difference between the two pixels the larger will be the number of secret bits that can be embedded. The small difference value indicates the block is in smooth area. The large difference value indicates the block is in edge area. The edge adaptive scheme in which the pixels in edge areas may tolerate larger changes of pixel values than those in the smooth area. It is possible to embed more data in edge area. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, a novel steganographic approach using multi-way pixel-value differencing is used. This will also reduce the quality distortion of stego-image brought from setting larger embedding capacity.

Index Terms: Steganography, Pixel-value differencing, Data hiding.

1. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images.

All digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree ofredundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

In practice two properties undetectability and embedding capacity should be considered when designing the steganographic algorithm. The larger the payload embedded in a cover, the more detectable artifacts would be introduced in the stego. The most important requirement is undetectability, which means that the stegos should be visually and statistically similar to the covers while keeping the embedding rate as high as possible.

The capacity and invisibility are the benchmarks needed for data hiding techniques of steganography. Due to the benchmarks, fragile schemes of data hiding are often used on steganography and least significant-bits (LSB) substitution is one of them. The scheme of least-significant-bits (LSB) substitution is a common

[1,2,3] Department of Computer Science and Engineering SRM University, India, *Emails: idaseraphim87@gmail.com, arul.sowmiya17@gmail.com, anijoe@gmail.com*

and well-known steganographic method. Embedded data are converted to substitute the fixed length LSB of each pixel. However, since some pixels cannot tolerate changes of substitution during the embedding process, then those pixels appear apparently different from their original values. This effect occurs seriously in the smooth area that those changes are noticeable for human eyes. Thus, improving the stego-image quality and adaptive adjusting hiding capacity are two major aims to expand related researches about LSB.

Two benchmarks are adopted by steganographic techniques to evaluate the hiding performance. First one is the capacity of hiding data and another one is the imperceptibility of the stego-image, also called the quality of stego-image. The pixel-value differencing (PVD) method proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image.

A novel steganographic approach using multi-way pixel-value differencing is proposed. To increase the hiding capacity of original PVD method referring to only one direction, more than onedifferent directional edge are considered and effectively adopted to design the multi-way differencing scheme. Also, to reduce the quality distortion of the stego-image brought from setting larger embedding capacity, an optimal approach of selecting the reference point and adaptive rules are presented. This can maintain the stego-image at an acceptable and satisfied quality.

2. RELATED WORK

Steganography is done either in spatial domain or in frequency domain. Spatial methods involve less complexity comparatively. Many methods have been proposed for embedding secret data in spatial domain. The most common method is called Least Significant Bit substitution (LSB). The secret data are converted to substitute the fixed length LSB of each pixel. However, since some pixels cannot tolerate changes of substitution during the embedding process, they appear apparently different from their original values. This effect is exhibited seriously in the smooth areas of the images and areeasily detected by some reported steganalytic algorithms, such as the Chi-squared attack, regular/singular groups (RS) analysis, sample pair analysis, and the general framework for structural steganalysis[13 - 16]. As a result, many new sophisticated LSB approaches have been proposed to improve this drawback, which use the concept of human vision to increase the quality of the stego-images.

The other category of spatial domain image steganography is the pixel-value differencing (PVD) method. Wu and Tsai [4] proposed a PVD steganographic method that uses the difference value between two neighbour pixels to determine how many secret bits should be embedded. The capacity of hidden data in edged areas is higher than that of smooth area. In this method difference between two neighbouring pixels is calculated and based on their difference secret data is embedded in to the pixels i.e. larger the difference, larger is the capacity of pixels to hold secret data. To further improve the quality of the stego-image, some PVD methods [10] were proposed, and these schemes utilized the HVS sensitivity to intensity variations from smoothness to high contrast by the selection of the width of the range which the difference value of two neighbour pixels belongs to. By combining the LSB insertion and PVD methods, Wu et al. [6] proposed a data hiding scheme with a better image quality by using PVD methods alone. In their approach, two consecutive pixels are embedded by the LSB replacement method if their difference value falls into a lower level; similarly, the PVD method is used if the difference value falls into a higher level. In other words, the secret data is hidden intothe smooth areas by LSB substitution and PVD methods in the edge areas.

From the analysis and the experimentation conducted, it is observed that a lot of approaches which attempt to embed data adaptively by considering the human vision sensitivity, offering high capacity and low distortion have been proposed. Anyways, some of them seemed not to provide competent payload capacities, and not completely follow the principle that the edge areas can tolerate more changes than smooth areas. Also the schemes that offer high payload capacity introduce detectable artifacts into the image and do not perform well in terms of the security or picture quality of the stego images.

3. THE PROPOSED METHOD

In the proposed system we will design a system in the spatial domain by using spatial domain methods that will enlarge the embedding capacity and to improve the perceptual transparency and to decrease the statistical undetectability a novel steganographic approach using multi-way pixel value differencing scheme will be designed.

To upgrade the hiding capacity of original PVD method referring to only one direction, different directional edges are considered and effectively adopted to design the scheme of multi-way pixel-value differencing. In addition, to reduce the quality distortion of stego-image brought from setting larger embedding capacity, an optimal approach of selecting the reference point and adaptive rules are presented. These schemes will provide superior embedding capacity and gives secrecy protection from dual statistical stego-analysis. Besides, the embedded confidential information can be extracted from stego-images without the assistance of original images.

Here the two aspects are evaluated they are imperceptibility and the hiding capacity. The differences between the stego and cover image must be imperceptible to the human eye. The higher the stego image quality the more invisible the hidden messages will be. The stego image quality that the human eye can accept can be judged by the Peak Signal-to-Noise Ratio (PSNR). A greater PSNR value indicates lower degree of image distortion after the hiding of secret message. The Capacity of embedding secret information will be increased and at the same time the imperceptibility of the stego and cover images will be maintained. The flow diagramfor embedding and extraction of the proposed system is as follows

3.1. Data Embedding

3.1.1. Pre-processing Phase

The cover image I of size $M \times N$ is first divided into non-overlapping blocks of $\square\square \Re_Q \times \Re_Q$ pixels. The size of the block is the $stego\_key_1$. Every small block is rotated by a random degree by an angle of $\{0^o, 90^o, 180^o, 270^o\}$. The angle of rotation θ, is the $stego\_key_2$. This random rotation step offers two advantages. Firstly, the security of the stego image is enhanced, i.e., the rotation key adds an additional level of security without which the detector cannot retrieve the correct hiding unit. Besides, both the horizontal and vertical edges present in the cover image are used for data embedding.

As shown in Fig. 2, each 2×2 block includes four pixels $P(x, y)$, $P(x, y + 1)$, $P(x + 1, y)$, and $P(x + 1, y + 1)$ where x and y are the pixel location in the image. The pixel pairs are formed as shown in the Figure 2.

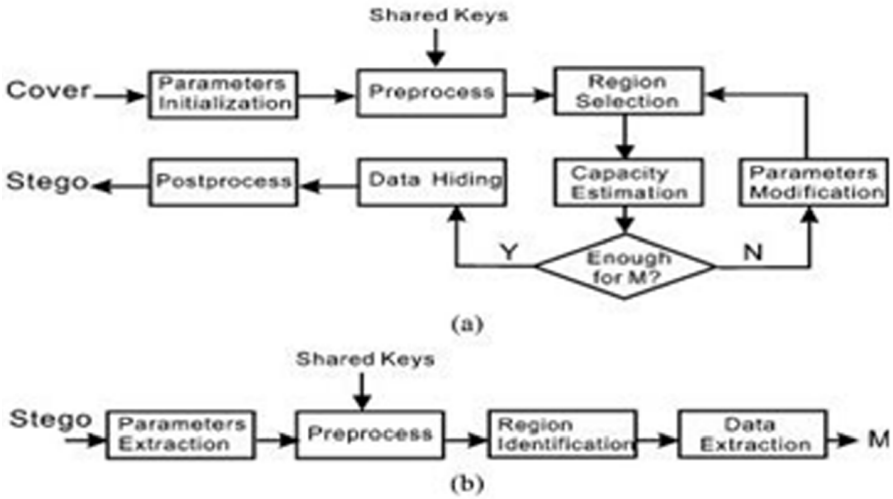

Figure 1: Proposed scheme. (a) Data embedding (b) Data extraction

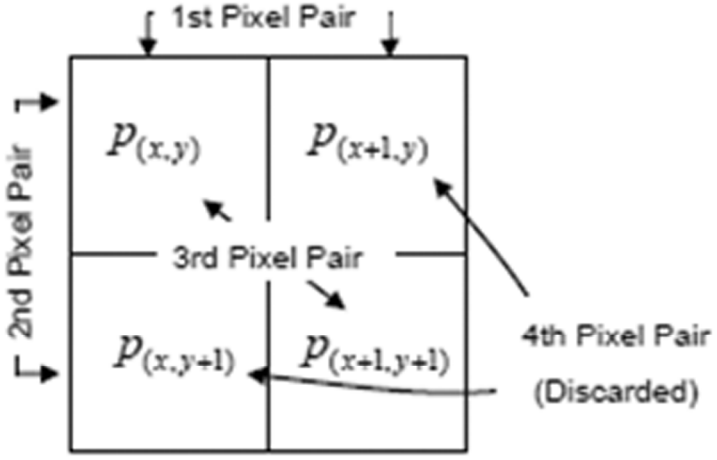

Figure 2: The pixel pairing scheme in the proposed system

3.1.2. Region Identification Phase

The regions in the cover image are to be identified as smooth and edge regions. This is decided based on a threshold value Δ, which can be decided as follows. Let $HU(\Delta)$ be the set of hiding units whose pixel pairs absolute differences are equal to or greater than a parameter β.

$$HU(\Delta) = \left\{ \left(p_i, p_j \right) \middle\| p_i - p_j \right| \geq \beta, \forall (p_i, p_j) \in HU \right\} \tag{1}$$

where p_i is the central pixel in each *HU* and *Pj* is its neighboring pixel in all the eight directions. Then the all the edge regions are selected as per the threshold Δ like

$$\Delta = \arg \max_{\beta} \left\{ 2 \text{ X } \left| \text{HU}(\Delta) \right| \geq \left| \text{MSG} \right| \right\} \tag{2}$$

where $\beta \in \{0, 1, ..., 31\}$, $|\text{MSG}|$ is the length of the secret binary message MSG, and $|HU(\Delta)|$ denotes the total number of hiding units satisfying the equation (1).

3.1.3. Range Table Construction Phase

Let I_i be the i^{th} sub block of *I* with the two horizontally or vertically or diagonally neighboring pixels denoted as $P(i, x)$ and $P(i, y)$. A range table *RT* containing n contiguous sub-ranges RTj has to be designed first. The main purpose of the range table is to provide adaptive hiding capacity for each I_i. The nature of the region of every neighboring pixel pair in each hiding unit is determined. Pairs belonging to the edge regions can hold more bits than the pairs belonging to non-edge regions. Thus the payload holding capacity of the every hiding unit is a variable one and the tolerable range of pixel modification t_i (number of bits to be embedded) is determined from this range table. Each sub-range RTj Rj has lower and upper bound values, *lj* and *uj* respectively, so that we have $\text{RTj} \in [lj, uj]$. Basically the width *wj*, computed as $wj = uj - lj + 1$, is selected to be a power of 2. Every single block *Ii* is mapped to its sub-range from the range table *R* such that $di \in [lj, uj]$. The value of *di* is obtained as:

$$di = \left| P(i, x) - P(i, y) \right| \tag{3}$$

The hiding capacity of the two pixels can be obtained by

$$ti = \left\lfloor \log_2 (wj) \right\rfloor \tag{4}$$

t_i is the number of bits that can be embedded in I_i. Read t_i bits from the binary data stream and transform t_i into decimal value b_j. If d_i is large, it indicates the pixel is in a high frequency region, i.e., it represents an edge position and can hold more bits. A smaller d_i value indicates the pixel value belonging to the smooth regions and non-edge regions and hence lesser payload hiding capacity. Table 1 show the Range Table employed in the proposed scheme.

Table 1
The Range Table used in the Proposed System

Index j	*Range[l u]*	*Hiding Capacity in Bits*
1	[0 7]	3
2	[8 15]	3
3	[16 31]	4
4	[32 63]	5
5	[64 127]	6
6	[128 255]	7

3.1.4. Multiway PVD Embedding Phase

Calculate the remainder values $I\text{rem}(i)$ from $\mathrm{P}(i,x)$, $\mathrm{P}(i,y)$ by the following equation:

$$I\text{rem}(i) = (P(i,x) + P(i,y)) \bmod \delta \tag{5}$$

where $\delta = 2^{t_i}$. Embed *ti* bits of secret message into *Ii* by altering $P(i, x)$ and $P(i, y)$. Compute new pixel values such that the new remainder $I\text{rem}(i) = (P(i,x) + P(i,y)) \bmod \delta$ equals the decimal value of message b_i to be embedded. The optimal approach to altering the $P(i, x)$ and $P(i, y)$ to achieve the minimum distortion as follows:

Case 1: $I_{rem(i)} > b_i$ *and* $m_i \le 2^{ti-1}$ *and* $P_{(i,x)} \ge P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} - \lceil m_i / 2 \rceil, \mathrm{P}_{(i,y)} - \lfloor m_i / 2 \rfloor);$$

Case 2: $I_{rem(i)} > b_i$ *and* $m_i \le 2^{ti-1}$ *and* $P_{(i,x)} < P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} - \lfloor m_i / 2 \rfloor, \mathrm{P}_{(i,y)} - \lceil m_i / 2 \rceil);$$

Case 3: $I_{rem(i)} > b_i$ *and* $m_i > 2^{ti-1}$ *and* $P_{(i,x)} \ge P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} + \lfloor n_i / 2 \rfloor, \mathrm{P}_{(i,y)} + \lceil n_i / 2 \rceil);$$

Case 4: $I_{rem(i)} > b_i$ *and* $m_i > 2^{ti-1}$ *and* $P_{(i,x)} < P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} + \lceil n_i / 2 \rceil, \mathrm{P}_{(i,y)} + \lfloor n_i / 2 \rfloor);$$

Case 5: $I_{rem(i)} \le b_i$ *and* $m_i \le 2^{ti-1}$ *and* $P_{(i,x)} \ge P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} - \lceil n_i / 2 \rceil, \mathrm{P}_{(i,y)} - \lfloor n_i / 2 \rfloor);$$

Case 6: $I_{rem(i)} \le b_i$ *and* $m_i \le 2^{ti-1}$ *and* $P_{(i,x)} < P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} + \lfloor n_i / 2 \rfloor, \mathrm{P}_{(i,y)} + \lceil n_i / 2 \rceil);$$

Case 7: $I_{rem(i)} \le b_i$ *and* $m_i > 2^{ti-1}$ *and* $P_{(i,x)} \ge P_{(i,y)}$

$$(\mathrm{P'}_{(i,x)}, P'_{(i,y)}) = (\mathrm{P}_{(i,x)} - \lceil m_i / 2 \rceil, \mathrm{P}_{(i,y)} - \lfloor m_i / 2 \rfloor);$$

Case 8: $I_{rem(i)} \le b_i and\ m_i > 2^{ti-1}\ and\ P_{(i,x)} < P_{(i,y)}$

$$(P'_{(i,x)},P'_{(i,y)})=(P_{(i,x)}-\lfloor m_i/2 \rfloor,P_{(i,y)}-\lceil m_i/2 \rceil);$$

where $m_i = \left| I_{rem(i)} - b_i \right|$ and $n_i = 2^{t_i} - m_i$. $P'(i, x)$, $P'(i, y)$ are new pixel values after embedding *ti* bits of secret message. Consider three situations when the pixels fall of the boundary limits. In such cases following steps should be executed accordingly so that pixel values $(P0j', Pj')$ lie within the boundary.

3.1.5. Falling-Off Boundary case

If the new pixel values $P'(i, x)$ and $P'(i, y)$ fall off the boundary $[0, 255]$, they can be revised by following the steps below. Consider three situations where the falling-off-boundary problem happens and revise $P'(i, x)$ and $P'(i, y)$ as follows:

Case 9: If $P_{(i,x)} \approx 0$ and $P'_{(i,x)} < 0$ or $P'_{(i,y)} < 0$,
then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be
$P'_{(i,x)} + (2^{ti}/2)$ and $P'_{(i,y)} + (2^{ti}/2)$.

Case 10: If $P_{(i,x)} \approx 255$, $P'_{(i,y)} \approx 255$ and $P'_{(i,x)} > 255$ or $P'_{(i,y)} > 255$,
then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be
$P'_{(i,x)} - (2^{ti}/2)$ and $P'_{(i,y)} - (2^{ti}/2)$.

Case 11: If $P_{(i,x)}$ and $P_{(i,y)}$ form a great contrast (i.e. d_i >128),
then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ as
if $P'_{(i,x)} < 0$ and $P'_{(i,y)} \ge 0$, then
$(0, P'_{(i,x)} + P'_{(i,y)})$;
if $P'_{(i,x)} \ge 0$ and $P'_{(i,y)} < 0$, then
$(P'_{(i,x)} + P'_{(i,y)}, 0)$;
if $P'_{(i,x)} \ge 0$ and $P'_{(i,y)} > 255$, then
$(P'_{(i,x)} + (P'_{(i,y)} - 255), 255)$;

After this step $P_{(i,x)}$ and $P_{(i,y)}$ can be corrected so that the pixel values lie within the range limits 0 and 255. Now these steps are to be done on every hiding unit of the image containing eight pixel pairs.

3.1.6. Post Processing Phase

After data hiding, the stego-image I' is constructed back by combining all the hiding units. The hiding units are then rotated by a random number of degrees based on $stego\_key_2$. The process is very similar to the preprocessing phase except that the random degrees are opposite. Now the stego-image looks very similar to that of the cover image but with the secret inside it.

3.2. Data Extraction

The process of extracting the embedded message is the same as the embedding process with the same traversing order of blocks. The stego-image I' is partitioned into 2 × 2 non- overlapping hiding units with

eight pixel pairs. Every hiding unit is rotated by random degrees based on the $stego\_key_1$. The same range table is referred for extraction. For each hiding unit, the detailed steps of data extracting are as follows.

1. Calculate the difference values $d'i$ separately for each sub-block $I_i^{'}$ using Eqn. 3.

   Each sub-block $I_i^{'}$ can be mapped to its sub-range Rj from the original range table R according to the difference value $d'i$

2. Compute the width of sub-range *wj* using $wj = uj - lj + 1$ and the number of bits *tj* of the secret data can be extracted from $I_i^{'}$ using Eqn. 4.

3. Calculate the remainder value $I'\text{rem}(i)$ using Eqn. 5 and convert into a binary string. This is the secret message embedded in $I_i^{'}$

4. Repeat the steps 2 to 5 until the entire message is extracted.

4. EXPERIMENTAL RESULTS AND DISCUSSION

For the evaluation of the proposed method, our cover image dataset consists of 1338 uncompressed color images with a size of 384 × 512 or 512 × 384 dimension, from UCID [40], 2000 images from [41] and NRCS image database [42] with categories like Portraits, Gardens, Architecture, Interiors, Macro, Studio, Underwater, Street photography, Aerial photography and Tourists having a wide range of image samples. These images portrayed sufficiently diverse nature for fair evaluation with good degrees of variation in texture, color, brightness and intensity. The RGB color images are converted to grayscale before data embedding.

5. CONCLUSION

In adaptive algorithms the embedding rate for each pixel of an image is determined by the humanvisual system. In these algorithms higher embedding rates are performed in the edge areas ofimages. Smooth regions are either left alone or lower embedding rates are performed in them. Ashort coming of the existing

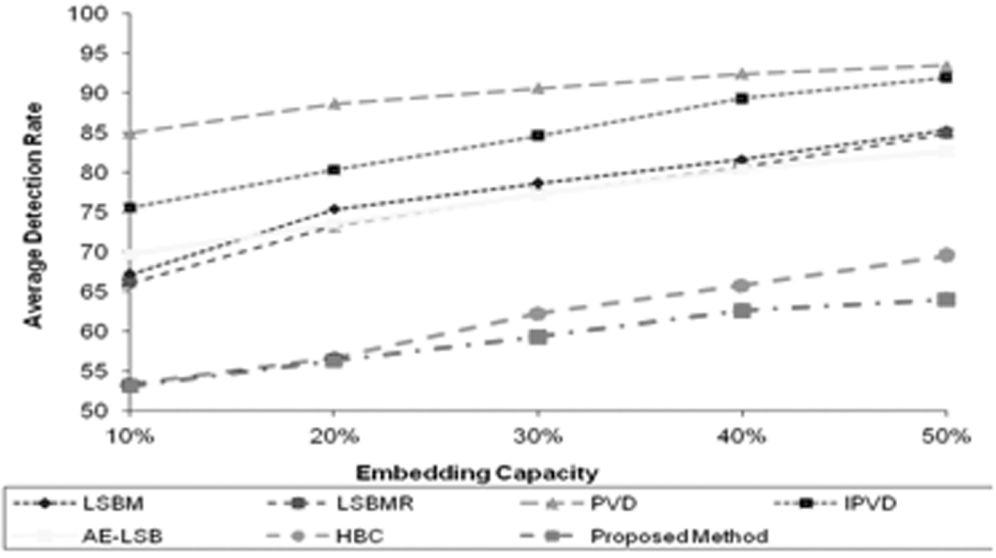

Figure 3: Average Detection Accuracy of various Steganographic schemes With wen-Nung 2-D Features

Table 2
Comparison Table

Cover-images (512 × 512)	*PVD method*		*Proposed Multiway PVD method*	
	Maximum Capacity (Bits)	*PSNR (dB)*	*Maximum Capacity (Bits)*	*PSNR (dB)*
Lena	529842	34.2124	803450	36.3779
Baboon	590299	29.9581	883516	33.3687
Airplane	536688	34.1044	811398	35.8205
Clown	533295	33.2515	814230	35.7228
Peppers	532985	33.5849	805893	36.4086
Barb	547163	31.7381	844967	34.5540
Zelda	525795	34.8050	794750	36.9496
House	536535	33.1630	817195	35.6285
Lighthouse	551633	31.6107	843291	34.6061
Pent	547056	32.0810	827290	35.2145
Boats	543566	33.3340	819282	35.4940
Truck	538632	33.4110	807352	36.2016
Kiel	567078	31.8961	850078	34.4228
Houses	571310	31.0346	873241	33.6253

adaptive algorithms is that they embed data using LSB routine.We eased this problem by embedding based on PVD algorithm. Furthermore, we presented acomplete scheme which identifies edges in the cover image and after altering the image byembedding data in it, allows the receiver to identify the exact same edges for the extractionpurposes. In future we are planning to extend it by using 8-neibgourhood pixels.

REFERENCES

[1] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis," IEEE Transactions on Signal Processing, Vol. 51, No. 7, pp. 1995-2007, 2003.

[2] M. Kharrazi, H.T. Sencar, and N. Memon, "Image steganography: concepts and practice," Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, 2004.

[3] B.Pitzmann, "Information hiding terminology," Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp. 347-350, 1996.

[4] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.

[5] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognition Letters, No. 3, pp. 331-339, 2004.

[6] T. C. Lu, and C. C. Chang, "Lossless nibbled data embedding scheme based on difference expansion," Image and Vision Computing, Vol. 26 , No. 5, pp. 632-638, 2008.

[7] Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis of pixel-value differencing steganographic method," IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 292-295, 2007.

[8] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis and payload estimation of embedding in pixel differences using neural networks," Pattern Recognition, Vol. 43, pp. 405- 415, 2010.

[9] S. S. Maniccam, and N. Bourbakis, "Lossless Compression and Information Hiding in Images," Pattern Recognition, Vol. 37, pp. 475-486, 2004.

[10] T. C. Liu, and C. C. Huang, "Lossless Information Hiding Scheme Based on Pixels Complexity Analysis," Proceedings of Third International Conference on Signal Image Technology & Internet-based Systems (SITIS 2007), Shanghai, China, pp. 934-941, 2007.