Secure Image Steganography Using Tri - Way Pixel - Value Differencing on Two Cover Images

ARCHANA O. VYAS[1], SANJAY V. DUDUL[2]
Department Of Applied Electronics
Sant Gadge Baba Amravati University
Amravati, Maharashtra
INDIA
nyasa.archana@gmail.com[1],svdudul@gmail.com

Abstract: - In tri – way pixel – value differencing(TPVD) steganography approach, three different directional edges of the cover image are considered to create a st ego image. TPVD gives more hiding capacity as compared to original pixel value differencing (PVD) method referring to only one direction. Encryption with steganography gives more secrecy protection to the system. In this paper, a more secure image steganographic technique is proposed, which includes encryption of image before embedding it in, two cover images using TPVD. Experimental results demonstrate that use of two cover images provide high embedding capacity. The peak signal to noise ratio (PSNR), mean square error (MSE) and hiding capacity are evaluated as performance parameter and found to have reasonable values as compared to previous related work. E ncryption before embedding protects the information from unauthorized access. The embedded confidential information can be retrieved from the stego images successfully without assistance of original images.

Key-Words: -Steganography, stego images, encryption, hiding capacity, TPVD, PVD, PSNR, MSE.

1 Introduction

To protect secret message from being stolen during transmission, there are two ways to solve this problem in general. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully; another way is steganography [1,9]. Steganography is an art of sending a secret message under the camouflage of carrier content. The carrier content appears to have totally different but normal ("innocent") meanings. The goal of steganography is to mask the very presence of communication, making the true message not discernible to the observer. The carrier image in steganography is called the "cover image" and the image which has the embedded data is called the "stego image". There are two kinds of image steganography techniques: spatial-domain and transform domain based methods. Spatial domain based methods embed messages directly in the intensity of pixels of images. For transform domain based ones, images are first transformed to another domain (such as frequency domain), and information is then embedded in transform coefficients [2].

One of the popular steganographic techniques is least-significant-bits (LSB) substitution, in which the least significant bits of the cover image are replaced with secret bits. Without loss of generality, LSB approaches usually obtain a considerably high capacity in addition to retaining good quality. Although LSB approaches are efficient with regard to capacity and image quality, the existence of embedded data is easily detected by bit planes or programs. Therefore, some hiding approaches are based on the concept of the human visual system and are different to the LSB approach [3]. Wu and Tsai proposed a pixel value differencing steganographic method that uses the difference value between two pixels in a block to determine how many secret bits should be embedded [4]. Recently, 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 [4] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. Therefore, based on PVD method, various approaches have also been proposed [5-6]. Chang and Huang [1] proposed a novel steganographic approach using tri-way pixel-value differencing (TPVD), to increase the hiding capacity of original PVD method referring to only one direction. In their approach,

three different directional edges are considered and they effectively adopted to design the tri-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 [1].

In this paper tri-way pixel value differencing scheme is proposed to embed the secret image in two cover images, to enhance the hiding capacity as compared to the conventional PVD method. To have a high security, the secret image is first encrypted using a key and then it is embedded in two cover images. Thus, a good quality stego image is obtained from which the original image can be retrieved successfully.

The rest of this paper is organized as follows. Section 2reviews the PVD method. In Section 3, the TPVD scheme is presented. Section 4 and 5 depict the embedding and extraction algorithm. Section 6 highlights the performance parameters to be evaluated. Experimental results are illustrated and in Section 7, prior to conclusions in Section 8.

2 Review Of The PVD Method

In the original PVD method [4], a gray-valued cover image is partitioned into non-overlapping blocks composed with two consecutive pixels, $p_i$and p_{i+1}. From each block, a difference value $d_i$can be calculated by subtracting p_i from p_{i+1}. The set of all difference values range from −255 to 255. Therefore, $|d_i|$ ranges from 0 to 255. Thus, the block with a small value $|d_i|$ locates in the smooth area, whereas a block with a large value $|d_i|$ is considered as a block with sharp edges. According to the properties of human vision, eyes can tolerate more changes in sharp-edge blocks than in smooth blocks. That is, more data can be embedded into the edge areas than into smooth areas. Therefore, in thePVD method, the first step is to design a range table with n contiguous ranges (R_k where $k = 1, 2\ldots., n$) and the table range is from 0 to 255. The lower and upper boundary of R_k are denoted by l_k and u_k, respectively, then $R_k \in [l_k, u_k]$. The width w_k of R_k is calculated by $w_k = u_k - l_k + 1$ and w_k decides how many bits can be hidden in two consecutive pixels. Since R_k is designed as a variable, the original range table is required to extract the embedded secret data, based on the consideration of security [4].

For the original PVD method [4], the secret data is assumed to be a long-bit stream and the cover image is a gray-level image. The embedding algorithm is described as follows:

1) The difference value d_i between two consecutive pixels p_i and $p_{i+1}$for each block in the cover image is calculated. The value is given by $d_i = p_{i+1} - p_i$.

2) $|d_i|$ is used to locate a suitableR_k in the designed range table, that is to compute $j = min_k(uk - |di(x,y)|)$ where$u_{k \geq} |d_i|$ for all $1 \leq k \leq n$. Then R_j is the located range.

3) The amount of secret data bits t is computed, that can be embedded in each pair of two consecutive pixels. The value t can be estimated from the width w_j of R_j, this can be defined by $t = [\log_2 w_j]$.

4) Read t bits from the binary secret data and transform the bit sequence into a decimal value b. For instance, if bit sequence = 101, then the converted value $b = 5$.

5) The new difference value d'_i is calculated, that is given by $d'_i = l_j + b$, if $d_i \geq 0$ or $d'_i = -(l_j + b)$ if $d_i < 0$ to replace the original difference d_i.

6) Modify the values of p_i and p_{i+1} by the formula:

$$(Pi, Pi+1) = \left(Pi - \left[\frac{m}{2}\right], Pi + 1\left[\frac{m}{2}\right]\right) \quad (1)$$

Where $m = d'_i - d_i$. Until now, to embed the secret data into the pixel pair $(p'_i, p'_{i+1})$is done by changing the values of p_i and p_{i+1}. Step 1-6 are repeated until all secret data are embedded into the cover image, then the stego-image is obtained [10].

During the phase of secret extraction, the original designed range table is required. Thes ame method in the embedding phase is used to partition the stego-image into pixel pairs. Then the difference value $d'^{\wedge}_i$ for each pair of two consecutive pixels $p^{\wedge}_i$ and $p^{\wedge}_{i+1}$ in the stego-image is calculated. Next, $|d^{\wedge}_i|$ is used to locate the suitable R_j in Step 2 during the embedding phase. Therefore, $b^{\wedge}$ is obtained by subtracting l_j from $|d^{\wedge}_i|$. If the stego-image is not altered, $b^{\wedge}$ is equal to b. Finally, $b^{\wedge}$ is transformed from adecimal value into a binary sequence with t bits, where$t = [\log_2 w_j]$.

3 Review Of Tri-way pixel value differencing method

In the PVD method, two horizontal and consecutive Pixels can only represent a vertical edge, but the edge can have different directions. This motivates researchers to improve the PVD method by considering three directions that is TPVD.

3.1 The Partition Pre-procedure [1].

Generally, the edges in an image are roughly classified into vertical, horizontal, and two kinds of diagonal directions. Motivated from the PVD method,using two-pixel pairs on on e directional edge can work efficiently for information hiding.

This should accomplish more efficiency while considering four directions from four two-pixel pairs. This can be implemented by dividing the image into 2×2 blocks. An example of such block is shown in Fig. 1 [1].

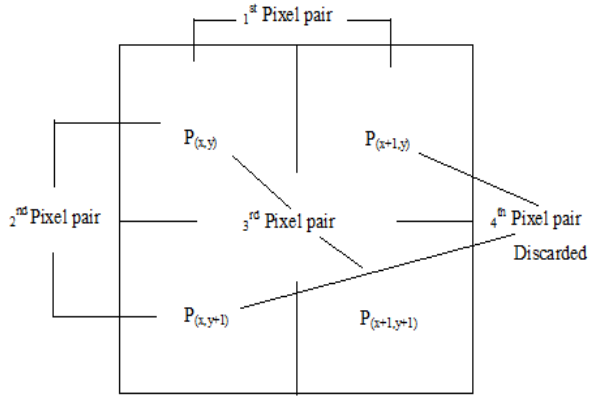

Fig. 1 An example of four pixel pair (block) [1].

However, since the changing of pixel values for the fourth pixel pair affects the first and the second pairs, the fourth pair is useless and has to be discarded. Therefore, three pairs are used to embed the secret data. It is required to partition the cover image into non-overlapping 2×2 blocks with 4 pixels. As shown in Fig. 1, each 2×2 block includes four pixels of $p_{(x,y)}$, $p_{(x+1,y)}$, $p_{(x,y+1)}$ and $p_{(x+1,y+1)}$ where x and y are the pixel location in the image. Let $p_{(x,y)}$ be the starting point, then three pixel pairs can be found by grouping $p_{(x,y)}$ with the right, the lower, and the lower right neighboring pixels. Those three pairs are named by p_0, p_1 and p_2, where, $p_0 = (p_{(x,y)},p_{(x+1,y)})$, $p_1 = (p_{(x,y)},p_{(x,y+1)})$ and $p_2 = (p_{(x,y)},p_{(x+1,y+1)})$ respectively [1].

When using the tri-way pixel value differencing (TPVD) method to embed the secret data in cover image, each pair of cover image has its modified p_i' and a new difference value d_i' for i = 0,1,2 . Now, the new pixel values in each pair are different from their original ones. That is, we have three different values for the starting point $p_{(x,y)}$ named $p_0'_{(x,y)}$, $p_1'_{(x,y)}$ and $p_2'_{(x,y)}$ from p_0, p_1 and p_2 respectively. However, only one value for $p_i'_{(x,y)}$ can exist after finishing the embedding procedures. Therefore, one of the $p_i'_{(x,y)}$ is selected as the reference point to offset the other two pixel values. That is, two pixel values of one pair are used to adjust the other two pairs and construct a new 2×2 block. Suppose that the reference point is $p_i'_{(x,y)}$, then the other two difference values, d_0' and d_2' can be proven unchanged after the adjustment given by

$$\begin{aligned} d_0'_{(x,y)} &= p_0'_{(x+1,y)} - p_0'_{(x,y)} \\ &= p_0'_{(x+1,y)} - p_0'_{(x,y)} + (p_1'_{(x,y)} - p_1'_{(x,y)}) \\ &= (p_0'_{(x+1,y)} - p_1'_{(x,y)}) - (p_0'_{(x,y)} - p_1'_{(x,y)}) \qquad (2) \\ d_2'_{(x,y)} &= p_2'_{(x+1,y+1)} - p_2'_{(x,y)} \\ &= p_2'_{(x+1,y+1)} - p_2'_{(x,y)} + (p_1'_{(x,y)} - p_1'_{(x,y)}) \\ &= (p_2'_{(x+1,y+1)} - p_1'_{(x,y)}) - (p_2'_{(x,y)} - p_1'_{(x,y)}) \qquad (3) \end{aligned}$$

The embedded secret data are unaffectedbecause of those three difference values are unaltered[1].

3.2 Optimal Selection Rules for the Reference Point[1].

Selecting different reference points results in varied distortion to the stego-image. Considering anoptimal selection approach to achieve minimum Mean Square Error (MSE). Suppose that $m_i = d_i' - d_i$ are the difference values of pixel pair i before and after embedding procedures. The rules that can exactly determine one optimal reference pair without really estimating MSE are introduced as follows.

1) If all values of m_i are greater than 1 or smaller than -1, the optimal pixel pair $i_{optimal}$ is the pair with thegreatest $|m|$. For example, if m_i = {-8, -4, -3}, $i \in$ {0, 1, 2}, then $i_{optimal}$= 0.

2) If all m_i have the same sign and only one $m_i \in${0, 1,-1}, then the optimal pixel pair $i_{optimal}$ is selected from the other two pairs with the smallest $|m|$. For example, if m_i={4, 3, 1}, $i\in${0, 1, 2} then $i_{optimal}$= 1.

3) If only one m_i has a different sign from the other two pairs, the optimal pixel pair $i_{optimal}$ is selected from the other two pairs with the smallest $|m|$. Forexample, if m_i={7,-4, 3}, $i\in${0,1, 2}, then $i_{optimal}$= 2.

4) If only one $m_i\in${0,1,-1} and the other two m_i has different signs, the optimal pixel pair $i_{optimal}$ is the pair with $m_i\in${0,1,-1}. For example, if m_i= {0,-4, 2}, if i = {0, 1, 2} then $i_{optimal}$= 0.

5) If there exists more than one pair with $m_i\in${0, 1,-1}, the optimal pixel pair $i_{optimal}$ can be selected as any one pair with $m_i\in${0, 1,-1} For example, if m_i = {4,0,0}, $i \in${0,1, 2} then $i_{optimal}$= 1 or 2.

4 Proposed embedding algorithm.

The details of proposed embedding algorithm are asfollows.

1) Read the cover image C_1 from the image database and display it on t he designed GUI.
2) Read the cover image C_2 from the image database and display it on t he designed GUI.
3) Calculate the hiding capacity of both cover images C_1, C_2 and display it on designed GUI.
4) Read the secret image to be embedded E_1 from the image database and display it on the designed GUI.

5) Choose a proper key and encrypt the secret image E_1, before embedding it into cover images using that key display the encrypted secret image on designed GUI.

4.1 ProposedTPVD method on two cover images

The tri-way pixel-value differencing method applied on selected two cover images is as follows.

1) Calculate four difference values $d_{i(x,y)}$ for four pixel pairs in each block of two cover images distinctly.
$$d_{0(x,y)} = p_{(x+1,y)} - p_{(x,y)} \quad (4)$$
$$d_{1(x,y)} = p_{(x,y+1)} - p_{(x,y)} \quad (5)$$
$$d_{2(x,y)} = p_{(x+1,y+1)} - p_{(x,y)} \quad (6)$$
$$d_{3(x,y)} = p_{(x+1,y+1)} - p_{(x,y+1)} \quad (7)$$
2) For both the cover images, Using $|d_{i(x,y)}|$ where (i =0,…,3) to locate a suitable $R_{k,i}$ in the designed range table, that is to compute $j = min_k(uk - |di(x,y)|)$ where $u_k \geq |d_i|$ for all $1 \leq k \leq n$. Then the located range can be represented by $R_{j,i}$.
3) Compute the amount of secret image data bits t_i that can be embedded in each pair by $R_{j,I}$ for the cover image C_1 and C_2. The value t_i can be estimated from the width $w_{j,i}$ of $R_{j,i}$, this can be defined by $t = [\log_2 w_{j,i}]$.
4) Read t_i bits from the binary secret image data and transform the bit sequence into a decimal value b_i.
5) Embed the secret image in cover image blocks according to the hiding capacity of two cover images.
6) Calculate the new difference value $d_i'_{(x,y)}$ given by $d_i' = l_{j,i} + b_i$ if $d_{i(x,y)} \geq 0$ $d_i' = -(l_{j,i} + b_i)$ if $d_{i(x,y)} < 0$ to replace the original difference $d_{i(x,y)}$ [1].
7) Modify the values of P_n and P_{n+1} by the followingformula for both the cover images C_1 and C_2.
$$(P'n, P'n+1) = \left(Pn - \left[\frac{m}{2}\right], Pn + 1 + \left[\frac{m}{2}\right]\right) \quad (8)$$
WhereP_n and P_{n+1} represent two pixels in P_i and $m = d'_n - d_n$. Until now, to embed the secret data into the pixel pair (P'_n ,P'_{n+1}) is done by changing theValues of P_n and P_{n+1}. Now, the new block is constructed from all pixel pairs and embedded with secret data is generated in both the cover images depending on the hiding capacity of the two cover images C_1 and C_2 , respectively.
8) Display the TPVD stego images on the designed GUI.
9) Calculate and display the values of MSE and PSNR.

5 Proposed extraction algorithm

To retrieve the embedded secret data from the TPVD stego image, the extraction algorithm is described in thefollowing steps.

1) Read the stego image SC_1 from the embedded image file and display it on the designed GUI.
2) Read the stego image SC_2 from the embedded image file and display it on the designed GUI.
3) Choose the same key for decryption, as that of encryption of the secret image E, so that the secret image can be obtained in its original form after de-embedding.

5.1 Proposed de-embedding method on two TPVD stego images.

The tri-way pixel-value differencing de-embedding method applied on two stego images is as follows.

1) Partition the two stego-images into 2×2 pixel blocks, and the partition order is the same as that in the embedding stage.
2) Calculate the difference values $d\hat{}_{i(x,y)}$ separately for each block in the two stego-images distinctly.
$$d\hat{}_{0(x,y)} = p_{(x+1,y)} - p_{(x,y)} \quad (9)$$
$$d\hat{}_{1(x,y)} = p_{(x,y+1)} - p_{(x,y)} \quad (10)$$
$$d\hat{}_{2(x,y)} = p_{(x+1,y+1)} - p_{(x,y)} \quad (11)$$
$$d\hat{}_{3(x,y)} = p_{(x+1,y+1)} - p_{(x,y+1)} \quad (12)$$
3) $|d\hat{}_{i(x,y)}|$ is used to locate the suitable $R_{k,i}$ as introduced in the embedding phase. At thesame time, the amount of embedding bits t_i, where $t_i = [\log_2 w_{j,i}]$ is obtained for the two stego images respectively.
4) $R_{k,i}$ is located, $l_{j,i}$ is subtracted from the selected $|d\hat{}_{i(x,y)}|$ and $b\hat{}_i$ is obtained. If the stego image is not altered, $b\hat{}_i$ is equal to b_i. Finally, $b\hat{}_i$ is converted from a d ecimal value into a binary sequence with t_i bits where $t_i = [\log_2 w_{j,i}]$.
5) Finally the de-embedded, decrypted recovered original secret image is displayed on the designed GUI.

6 Performance Parameters

The performance parameters that are required to be evaluated after TPVD steganography are described as follows.

6.1 Peak-Signal-to-Noise Ratio (PSNR)

As a p erformance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego-images. It is defined as in equation (13)

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE})dB \quad (13)$$

Where MSE denotes Mean Square Error which is given in equation (14),

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(X_{ij} - Y_{ij})^2 \quad (14)$$

Where *i* and *j* are the image coordinates, *m* and *n* are the dimensions of the image, Y_{ij} is the generated stego image and X_{ij} is the cover image. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious [7, 11].

6.2 Hiding Capacity

The embedding capacity or hiding capacity is the maximum number of bits that can be embedded in a given cover image. It is considered as the size of data embedded within cover image. It is the amount of information that can be hidden within the cover image without deteriorating the quality of cover image. It is given in bits or kilo bits. [8, 12]

7 Experimental Results

The proposed algorithm is tested in MATLAB programming environment. Fig. 2 d epicts the various secret images that are converted to gray image before hiding in two cover images.

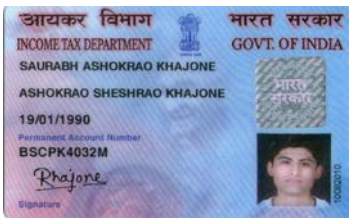

Fig.2. various secret images: Moon, Orange, Grapes, House and PAN card

Fig. 3(a) shows a GUI that is used to select two cover images “lena” and “girl”, select the secret image “moon” from the image database. It shows the encryption of secret image moon. It also shows the two stego images obtained after embedding encrypted secret image “moon” in two cover images “lena” and “girl”. The chosen encryption key is displayed on GUI. The PSNR, MSE during embedding process and hiding capacity of the two cover images are also evaluated and displayed on GUI.

Fig. 3 (b) depicts a GUI that is used to show the two stego images and two cover images. There is hardly any difference in the original cover images and the stego images; it indicates that image quality is not degraded after embedding a secret image “moon” in two cover images. When the same key as t hat of encryption key is used, the GUI shows the recovered original image “moon”. This indicates the faithful recovery of actual secret image without any loss in image content. The evaluated MSE, PSNR during de-embedding process and decryption key is displayed on GUI.

Fig. 4(a), Fig. 4(b), Fig.5 (a), Fig.5 (b), Fig. 6(a), Fig. 6(b), Fig.7(a), Fig.7(b) demonstrated the experimental results for the secret image “orange”, “grapes”, “house” and “PAN card”, respectively. PSNR values obtained for these images are 57.24dB, 63.44dB, 61.67dB and 61.34dB, respectively. For these secret images, the parameters such as MS E and PSNR are evaluated for embedding as well as de-embedding process; and hiding capacity values in kilo bits for two cover images are displayed on G UI.The experiment is conducted over a database of 100 images and it is observed that PSNR values obtained range from 57.2418 dB to 63.4453dB exhibiting satisfactory quality of images without significant loss of information.

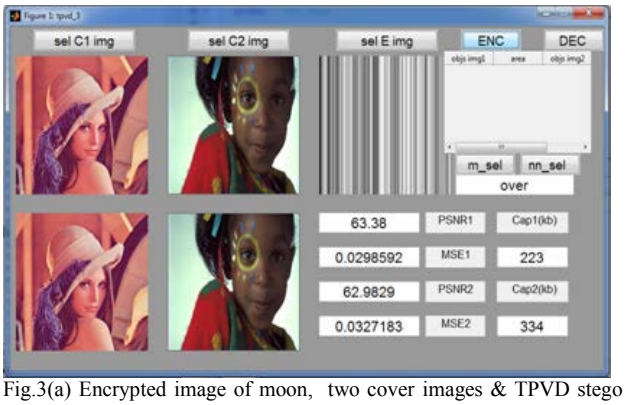

Fig.3(a) Encrypted image of moon, two cover images & TPVD stego images.

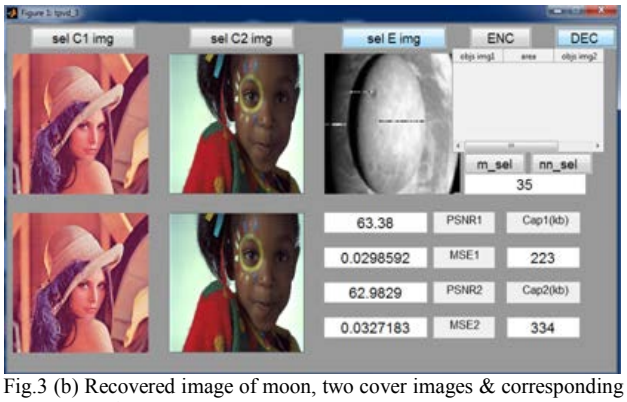

Fig.3 (b) Recovered image of moon, two cover images & corresponding TPVD stego images

Fig.4 (a) Encrypted image of orange, two cover images & TPVD stego images.

Fig.4 (b) Recovered image of orange, two cover images & corresponding TPVD stego images

Fig.5 (a) Encrypted image of grapes, two cover images & TPVD stego images.

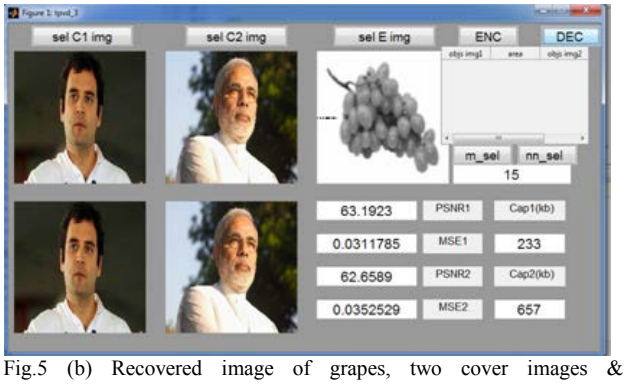

Fig.5 (b) Recovered image of grapes, two cover images & corresponding TPVD stego images

Fig.6 (a) Encrypted image of house, two cover images & TPVD stego images.

Fig.6 (b) Recovered image of house, two cover images & corresponding TPVD stego images

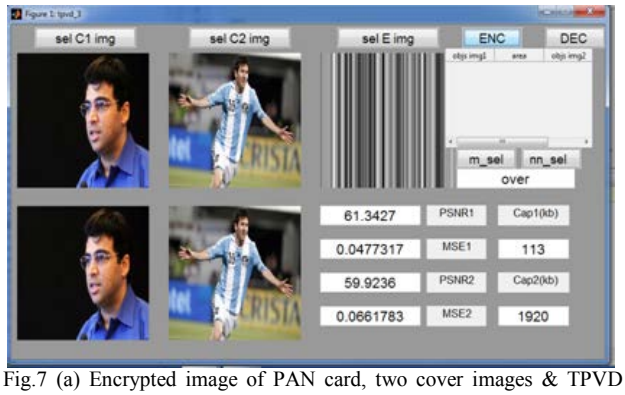

Fig.7 (a) Encrypted image of PAN card, two cover images & TPVD stego images.

PSNR, MSE and hiding (embedding) capacity for the tested secret images for corresponding cover images displayed in Fig. 3(a), Fig. 4(a), Fig. 5(a), Fig. 6(a) and Fig. 7(a) are shown in the following Table 1.

Table 1 MSE, PSNR and Hiding capacity for TPVD on two cover images during embedding a secret image.

Secret image	Cover image 1			Cover image 2		
	MSE	PSNR in dB	Hiding Cap.	MSE	PSNR in dB	Hiding Cap.
Moon Key 35	0.02985	63.38	223	0.03271	62.9829	334
Orange Key 25	0.12271	57.2418	337	0.21531	54.8	222
Grapes Key 15	0.02941	63.4453	233	0.03327	62.9099	657
House Key 20	0.04418	61.6783	2535	0.03753	62.3861	215
PAN card Key 55	0.04773	61.3427	113	0.06617	59.9236	1920

Similarly, the aforementioned performance parameters for the corresponding recovered (decoded) images portrayed in Fig. 3(b), Fig. 4(b), Fig. 5(b), Fig. 6(b) and Fig. 7(b) are shown in the following Table 2.

Table 2 MSE, PSNR and Hiding capacity for TPVD on two cover images during decoding the same secret image by same key.

Secret image	Cover image 1			Cover image 2		
	MSE	PSNR in dB	Hiding Cap.	MSE	PSNR in dB	Hiding Cap.
Moon Key 35	0.02985	63.38	223	0.03271	62.9829	334
Orange Key 25	0.12271	57.2418	337	0.21531	54.8	222
Grapes Key 15	0.03117	63.1923	233	0.03525	62.6589	657
House Key 20	0.04350	61.7457	2535	0.03835	62.2929	215
PAN card Key 55	0.04730	61.382	113	0.06656	59.8982	1920

As depicted by above experimental results, the PSNR values obtained during embedding and de-embedding are same for the secret image ‘moon’ and ‘orange’. PSNR values for secret image ‘grapes’ are reduced by 0.2530 dB for Cover image 1 and 0.2510 dB for cover image 2 during de-embedding

Fig.7 (b) Recovered image of PAN card, two cover images & corresponding TPVD stego images

as compared to their respective values during embedding for cover images C_1 and C_2 respectively. Similarly,there is hardly any significant loss of PSNR with respect to embedding and de-embedding (decoding) of secret images ‘house’ and ‘PAN card’. In addition, it is also noticed that the value of PSNR expressed in dB is over 61 dB entailing reasonable quality of the image. The maximum hiding capacity of 2535 K b is observed for cover image ‘Sachin’ as shown in Fig. 6 (b). It is also obvious from Tables 1 and 2 that the lower values of MSE yield higher values of PSNR indicating negative correlation between these two parameters. However, it is also seen that high value of PSNR does not ensure high value of hiding capacity.

8 Conclusion

We have thus implemented a novel method to hide the secret image in two distinct cover images using TPVD. The implementation is on two colour cover images. To impart more security to this method of steganography, encryption technique is applied on the secret image before it is embedded within the cover image.The method is tested on a database of 100 images and PSNR value obtained is quite satisfactory. The method is found successful with different encryption key on secret images applied on secret image to hide it in two cover images. We have successfully recovered the hidden image using the same key for decryption. A satisfactory high value up to 63.44dB of PSNR and high embedding capacity is thus obtained. MSE and PSNR are also evaluated after de-embedding procedure. Use of two cover images and encryption before embedding enhance the hiding capacity and security of the system as compared to the previous methods applied on a single cover image as reported in the literature.

9 Applications

The applications of the proposed steganography technique could be in hiding the confidential data and transmitting it using two cover images via different channel. The proposed scheme can be used in "digital certificate document system". The technique is also applicable for selective extraction of information by a p articular user, accessing a website, who knows the decryption key.

References:

[1] Ko-Chin Chang, Chien-Ping Chang, A Novel Image Steganographic Method UsingTri-way Pixel-Value Differencing, *Journal of Multimedia,* VOL. 3, NO. 2, JUNE 2008.

[2] Vajiheh Sabeti, Shadrokh Samavi, Shahram Shirani, Steganalysis of Pixel-Value Differencing Steganographic Method, *IEEEPacific Rim Conference On Communication and Computer Signal Processing*, 2007.

[3] Cheng-Hsing Yang, Shiuh-Jeng Wang,Analyses of Pixel-Value-Differencing Schemes with LSB Replacement inStegonagraphy, *IEEEThirdInternational Conference Intelligent Infermation Hiding and multimedia Signal Processing*, 2007.

[4] Wu. D.C., Tsai. W.H., A Steganographic Method for Images by Pixel-Value Differencing, *PatternRecognition Letters*, Vol. 24, No. 9-10. (2003) 1613.

[5] 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 on Vision, Image and Signal Processing*, Vol. 152, N o. 5, pp. 611-615, 2005.

[6] S.L. Li, K.C. Leung, L.M. Cheng, and C.K. Chan,Data Hiding in Images by Adaptive LSB SubstitutionBased on the Pixel-Value Differencing, *First InternationalConference on Innovative Computing, Information andControl (ICICIC'06)*, Vol. 3, pp. 58-61, 2006.

[7] Sandipan Dey, Ajith Abraham, Sugata Sanyal, An LSB Data Hiding Technique Using Prime Numbers,*IEEE, Third International Symposium on Information Assurance and Security*, 2007.

[8] Sumeet Kaur, Savina Bansal and R. K. Bansal,Steganography and Classification of Image Steganography Techniques, *IEEE International Conference on Computing For Sustainable Global Develpoement (INDIACom)*, 2014, 978-93-80544-12-0/14.

[9] EI sayed M., EI Alfy, Improved Pixel Value Differencing Steganography using Logistic Caotic maps, *IEEE International Conference On innovations in information technology, 2012.*

[10] Liping Ji, Xialong Li, A Further Study on a PVD Based Steganography, *IEEE International Conference on multimedia information networking and security, 2010.*

[11] Avinash Tyagi, Ratnakirti Roy, High Capacity Image Steganography Based on P ixel Value Differencing and Pixel value Sum, *IEEE, Second International Conference on Computing and Communication Engineering, 2015.*

[12] Mohit Rajput, Maroti Deshmukh, A Novel Approach for Concealing Image by Utilizing the Concept of Secret sharing Scheme and Steganography, *IEEE, International Conference on Information Technology (ICIT) 2016.*