REINFORCE IMAGE STEGANOGRAPHY FOR INFORMATION HIDING USING CWSSIM

V.V. Vinoth
Research Scholar
Department of ECE
Bharath University, Chennai
India
E-mail:vinothvv.velaian@gmail.com

Dr. B. Karthik
Associate Professor
Department of ECE
Bharath University, Chennai,
India
E-mail: karthik.ece@bharathuniv.ac.in

***Abstract*— In this paper, an image steganography approach is presented dividing the cover image into 2×2 non-overlapping pixel blocks. The upper-left pixel of that block embeds a certain number of bits of the secret bit stream. Whereas, the remaining pixels of the same block embed the secret data using a modified version of the pixel-value-differencing (PVD) method that considers embedding secret data into both horizontal and vertical edges; unlike traditional image steganography approaches. The experimental results show that the proposed approach perceptually outperforms competing approaches in terms of the standard PSNR and the complex wavelet SSIM index. In turn, the imperceptibility of the stego-image is improved with a comparable bit- embedding capacity.**

***Index Terms*—Steganography, Wavelet, Cryptography**

I.INTRODUCTION

Image processing is a particular procedure for accomplishing to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features connected with that image. A digital image is a something in a particular way ofa two-dimensional image as a finite set of digital values, called picture elements or pixels. Pixel values typically constitute gray levels, colors, heights, opacities etc.

Information security is the series of actions of protecting the intellectual property of an organization. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation, although it may also involve reducing the adverse impacts of incidents. It has attracted agreat attention in the past few decades due to its importance in the growing communication field. Various cybercrimes such a forgery, modification, duplication and interception have reached alarming levels. So, information security issue requires immediate and reasonable solutions, such as cryptography and/or steganography. Cryptography is a well-known solution to protect data using the concept of encrypting the message to become unreadable. Encrypting digital media,such as audio,image, video successfully bring about higher secrecy performance. However ,such encrypted media become, then, attractive to eavesdroppers (*i.e.*, information attackers) as the encrypted media are presented in a perceptible manner. Instead, steganography can be considered as an alternative to overcome the perceptibility issue.

The main aim of the steganography process is to conceal the information being transferred within some digitally covered media avoiding the attention of eavesdroppers. Steganography is acquired from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the facts provided is hidden exclusively in images. Extremely difficult to discern, a normal cover message was sent over an not firm channel with one of the periods on the paper containing hidden information. This makes steganography a good manner to communicate secret information through digital cover media, such as audio, image, video, text *etc*.

Steganography process has many challenges due to transferring secret text information within a digitally covered media [1]. The main challenge is to transfer a higher size of secret text information within a limited image size without changing the imagequality; at least to the human visual system. The desired attributes of Steganography are

- Imperceptibility
- Capacity
- Robustness

Therefore, the steganography process is a trade-off problem. The steganography process can be performed in either frequency domain orspatial domain. In the frequency domain, the joint photographicexperts group (JPEG) format is frequently used, due to its small size being easily transferred on the internet. After changing the *RGB* color representation to the Y *U V* representation, the color component, *V,* can be then down sampled to decrease the file size. In turn, the resulting image file is transformed using the discrete cosine transform (DCT), or the discrete Fourier transform (DFT). Finally, the transformed image is compressed with a lossless Huffman encoding. As the DCT and quantization steps are lossy, the secret text information using the least significant bit (LSB) embedding step can be performed right before the Huffman encoding step, yielding a stego-image [2].

Whereas, in [3], [4], authors use sparse decomposition of one level using the Haar wavelet transform to hide text information within non-overlapping blocks in combination with the LSB-based substitution method with becoming greater in size the transmission capacity on the secret messages perceptibility in the stego-image.

In the spatial domain-based approaches, the steganography process is performed by generating the LSB-based substitution matrices. Then, the secret text information is distributed among all pixels in a gray-scale or colored image; the digitally covered media. Finally, the stego-image is generated with a certain image quality. So, the spatial domain-based ap- proaches can be partitioned into three categories: (i) high embedding capacity approaches with barely acceptable image quality (*e.g.*, [5]–[7]), (ii) high image quality approaches with reasonable hiding capacity (*e.g.*, [8]–[10]), and (iii) restricted embedding capacity approaches with a slight distortion in the image (*e.g.*,[11]–[13]).

In [11] authors use the optimal pixel adjustment procedure (OPAP) in combination with a modified Hamming method to improve the imperceptibility of the stego-image, however, with a limited size of the hidden text. In [12], an adaptive LSB substitution method using lacking a mutual relationship color space, increasing the property of imperceptibility to embed the encrypted data inside the *V* -plane of HSV color model based on secret key. Encryption is performed to sensitive contents using iterative magic matrix-based encryption algorithm.

In [10], an image steganographic method is presented based on the LSB substitution with a typical pixel value differencing (PVD) method, a modified version of PVD method, and an 8-neighboring (8nPVD) method, respectively, for gray-scale cover image in order to improvethe embedding capacity with a reasonable imperceptible stego-image. In [13], the image is partitioned into 2×2 pixel blocks in a non-overlapping fashion and scanned in raster-scan order having correlated the left- upper and bottom-right corner pixels. Although both horizontal and vertical edges a reconsidered in the approach of[13],more bit-hiding capacity is achieved at the cost of image quality. The construction of CW-SSIM has some interesting connections with several computational models that account for a variety of biological vision behaviors. T hese models include:

1) The involvement of band pass visual channels in image pattern recognition tasks.
2) The representation of phase information in primary visual cortex using quadrature pairs of localized bandpass filters.
3) The computation of complex valued product in visual cortex.
4) The computation of local energy (using sums of squared responses of quadrature pair filters) by complex cells in visual cortex.
5) The divisive normalization of filter process (using summed energy of neighboring filter responses)in both visual and auditory neurons.

CW-SSIM has been shown to be a useful measure in a series of applications, including

1) Image quality assessment
2) Line-drawing comparison
3) Segmentation comparison
4) Range-based face recognition
5) Palm print recognition

Although, those aforementioned approaches have reached a reasonable level of information hiding, all resulting stego-images are highly perceptible, thus assuring the existence of hidden information and attracting eavesdroppers. In this paper, we propose a spatial-based image steganography approach to hide text information with higher imperceptibility to avoid the information attackers. Unlike conventional approaches, the proposed approach makes use of hiding secret information in both horizontal and vertical edges with enhancing the visual quality of the stego-image, thus achieving higher imperceptibly. The proposed approach exploits the LSBMR method in combination with the optimal-pixel-adjustment process (OPAP) method to embed secret data into the cover images. In the embedding step of the proposed approach, the cover image is partitioned into non-overlapping 2×2 pixel blocks. The upper-left pixel is embedded with *k*-bits of the secret data using the LSB substitution method and is adjusted accordingly by the OPAP method to recover data on the recipient. Each of the other three pixels is then embedded with a certain number of bits using the LSBMR method. In the second stage, the data is extracted from stego-image. The rest of this paper is structured in a systematic way as follows. In Section II, the proposed spatial-based image steganography approach is presented using a modified version of the PVD method in combination with both the LSBMR and OPAP methods. Section III presents the performance evaluation metrics, implementation setup of competing approaches and the experimental results. Finally, conclusions are given in Section IV.

II.THE PROPOSED APPROACH

This section presents the proposed image steganography approach for gray-level cover image with a modified PVD method. The embedding and extraction steps are shown in Section II-A and Section II-B, respectively.

A.The Proposed Embedding Step

In the proposed embedding step of the proposed approach, the cover image is divided into 2×2 non-overlapping pixel blocksin a raster scan order. The modified PVD method divides the grey level range [0,255] into only six sub ranges, such that

R_1=[0,7], R_2=[8,15], R_3=[16,31], R_4=[32,63], R_5=[64,127], and R_6=[128,255].

Note that the modified PVD method, sub ranges R_1through R_4 are categorized as a lower gray-level, whereas the sub rangesR_5 andR_6 are categorized as a higher gray-level. Given that the sub range of gray level is R_j=[L_j,U_j], where j=1,2,3….6, its width can be cast as W_j=U_j-L_j+1. Also note that the maximum number of bits, t_j, to be embedded in the pixel pair is determined, such that t_j=a_1,a_2,a_3,a_4,a_5, and a_6 for R_j=R_1,R_2,R_3,R_4,R_5, and R_6 respectively. Also, note that the first pixel (i.e., the upper-left pixel) can be referred to B_{ib} as the base point of block *i.* As well the second pixel, B_{i2}, the third pixel, B_{i3}, and the fourth pixel, B_{i4} , can be referred to as the upper-right pixel, the bottom-left pixel, and the bottom-right pixel, respectively. The method of hiding a secret bit –stream into non-overlapping blocks is as follows:

1) Convert the *k* LSBs of $B_{ib}$to decimal,w_i.

2) Replace the *k* LSBs with the *k* leftmost secret bits to obtainB^n .

3)Determine the decimal value $v_i$for *k* bits from the secret bit-stream.

4)Determine the difference value: $d = w_i - v_i$.

5) UpdateB^n_{ib} , suchas

$$B^n_{ib}=\begin{cases} B^n_{ib}+2^k, if\ d>2^{k-1}\ and\ B^n_{ib}+2^k\le 255 \\ B^n_{ib}-2^k, if\ d<-2^{k-1}\ and B^n_{ib}-2^k\le 255 \\ B^n_{ib}, \qquad otherwise \end{cases} \quad (1)$$

6) Determine the difference between the second pixel,Bi2, of the pixel block and $Bib\ n$ as, Di1 =| Bi2 − $Bib\ n$ |

7) Determine he difference between the third pixel,Bi3, of the pixel block and $Bib\ n$ as, Di2 =| Bi3 − $Bib\ n$ |.

8)Determinethedifferencebetweenthefourthpixel,Bi4, of the pixel block and $Bib\ n$ as, Di3 =| Bi4 − $Bib\ n$ |.

9) For the differences, Di1, Di2 and Di3, find the corresponding sub ranges as shown above in this subsection. Then, find out the corresponding number of bits to be hidden from the secret bit stream; ti1, ti2 and ti3 as well as their lower bound; Li1, Li2 and Li3.

10) Having read the ti1, ti2 and ti3 bits from the secret bit stream, determine their decimal values; vi1, vi2 and vi3, respectively.

11)Determine the new difference values ,$D_1{}^n$,$D_2{}^n$,and $D_3\ n$, such as

$$D_1^n = L_{i1} + v_{i1}, D_2^n = L_{i2} + v_{i2}, D_3^n = L_{i3} + v_{i3}. \quad (2)$$

12) The new values,$Bi2\ n2$, $Bi2\ n3$,$Bi3\ n2$, $Bi3\ n3$

$$B^{n2}_{i2} = B^n_{ib} - D^n_1, \qquad B^{n3}_{i2} = B^n_{ib} + D^n_1,$$
$$B^{n2}_{i3} = B^n_{ib} - D^n_2, \qquad B^{n3}_{i3} = B^n_{ib} + D^n_2, \quad (3)$$
$$B^{n2}_{i4} = B^n_{ib} - D^n_3, and\ B^{n3}_{i4} = B^n_{ib} + D^n_3$$

13) Determine the difference values

$$d^{n2}_{i2} = |B_{i2} - B^{n2}_{i2}|, \qquad d^{n3}_{i2} = |B_{i2} - B^{n3}_{i2}|,$$
$$d^{n2}_{i3} = |B_{i3} - B^{n2}_{i3}|, \qquad d^{n3}_{i3} = |B_{i3} - B^{n3}_{i3}|, \quad (4)$$
$$d^{n2}_{i4} = |B_{i4} - B^{n2}_{i4}|, \qquad d^{n3}_{i4} = |B_{i4} - B^{n3}_{i4}|,$$

14) Determine the new value of the second pixel ,$Bi2^n$, such as

$$B^n_{i2} = \begin{cases} B^{n2}_{i2}, & if\ d^{n2}_{i2} < d^{n3}_{i2}\ and\ 0 \le B^{n2}_{i2} \le 255 \\ B^{n3}_{i2}, & otherwise \end{cases} \quad (5)$$

15) Determine the new value of the third pixel, $Bi3\ ^n$ such as

$$B^n_{i3} = \begin{cases} B^{n2}_{i3}, & if\ d^{n2}_{i3} < d^{n3}_{i3}\ and\ 0 \le B^{n2}_{i3} \le 255 \\ B^{n3}_{i3}, & otherwise\ . \end{cases} \quad (6)$$

16) Determine the new value of the fourth pixel, $Bi4\ ^n$,uch as

$$B^n_{i4} = \begin{cases} B^{n2}_{i4}, & if d^{n2}_{i4} < d^{n3}_{i4}\ and\ 0 \le B^{n2}_{i4} \le 255 \\ B^{n3}_{i4}, & otherwise \end{cases} \quad (7)$$

The same steps above should be repeated for all neighboring pixels of each pixel block to obtain a stego-block. Then, all stego-blocks form the stego-image, until all secret bits have been hidden.

B.The Proposed Extraction Step

In the proposed extraction Step of the proposed approach, the stego-image is divided into 2×2 non-overlapping blocks by scanning the image in a raster scan order. Note that the first pixel (i.e., the upper-left pixel) can be referred to $Bib\ n$ as the base point of the stego-block i. As well, the second pixel,$Bi2\ n$,the third pixel,$Bi3\ n$,and the fourth pixel,$Bi4\ n$,can be referred to as the upper-right pixel, the bottom-left pixel, and the bottom-right pixel, respectively. The method of extracting the secret bit-stream from the non-overlapping stego-blocks is asfollows:

1) Extract the k-rightmost LSBs of the pixel $Bib^{\ n}$,and name itv_{ib}.

2) Determine the difference values, such as

$$d_{i1}^n = |B_{i2}^n - B_{ib}^n|, d_{i2}^n = |B_{i3}^n - B_{ib}^n|, d_{i3}^n = |B_{i4}^n - B_{ib}^n| \quad (8)$$

3) Find out the appropriate range Rj , for the difference values $di1\ n$, $di2\ n\ and\ di3\ n$ from the sub ranges$R1$ through $R6$ as listed in Section II-A. Then, determine the corresponding values $ti1$,$ti2\ and\ ti3$given their lower bounds, such as $Li1$, $Li2\ and\ Li3$ respectively.

4) Extract the $ti1$,$ti2\ and\ ti3$ rightmost LSBs of the difference values $di1\ n$, $di2^{\ n}\ and\ di3\ n$ respectively.

5) Determine and concatenate a segment of the secret bit stream such as

$si1 = di1^{\ n} - Li1$, $si2 = di2^{\ n} - Li2\ and\ si3 = di3^{\ n} - Li3$.

Repetition of the above procedure for each stego-block will give the exact retrieval of the secret bit stream.

III.PERFORMANCE EVALUATION & EXPERIMENTALRESULTS

This section presents the evaluation metrics and the experimental results of the proposed image steganography approach compared to competing approaches shown in [10] and [13]. A set of standard gray-level images [14] with a different sizes have been chosen as cover images to check on the effectiveness of the competing approaches. Whereas, the secret image is taken in gray level square dimension. Note that our main aim in this paper is to enhance the imperceptiblity (i.e., improve the image visual quality) of the stego-image with hiding a secret bit-stream of higher capacity. Therefore, three performance metrics are used to evaluate the performance of the competing image steganography approaches: 1) The embedding capacity in bits on the basis of the higher the better. 2) The stego-image visual quality using both the standard peak-signal-to-noise(PSNR) ratio (in dB) [15, Ch. 3]on the basis of the higher the better. 3) The complex wavelet structural similarity (CWSSIM) index [16] is used, where 1 is a perfect match and 0 is a mismatch. Normally the more the embedding capacity using an image steganography approach, the lower the perceptual image quality. In turn, the image distortions occurred are slight and imperceptible. Table I shows the embedding capacity (in bits) as well as shows that the proposed approach outperforms the approaches shown in [10] and [13], by an average of 1.4 dB and0.9 dB, respectively, in terms of the standard PSNR value. As well, the proposed approach surpasses the competing approaches by an average of 11.6% and 8.5% in terms of the CWSSIM index. In addition, Table I shows that the bit-embedding capacity using the proposed approach outperforms the approach in [10] by an average increase of 13.6%. While the proposed approach is comparable to that in[13]. Given the experimental results, one can notice that the stego-image using the proposed approach perceptually seems the same as the original one. Thus, the eavesdropper's avoidance can be achieved incase that nonstandard Web-image has been used as a cover image instead of those standard images used. We can analyze that this enhancement is due to considering both horizontal and vertical edges, not only either of them as shown in competing approaches.

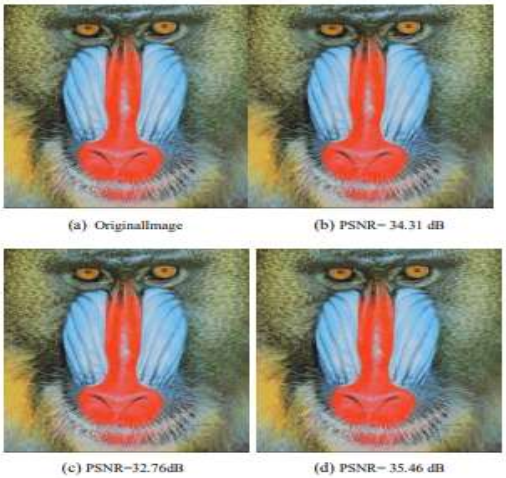

Fig. 1.(a) The standard cover image of Baboon, (b) the stego-image using the approach in [10], (c) the stego-image using the approach in [13], and (d) the stego-image using the proposed approach.

IV. CONCLUSIONS

In this paper, we present an image steganography approach dividing the cover image into 2×2 non-overlapping pixel blocks. The upper-left pixel of that block embeds a some but not all number of bits of the secret bit stream. Whereas, the remaining pixels of the same block embed data using a modified version of the pixel-value-differencing (PVD) method that considers embedding secret data into both horizontal and vertical edges. The experimental results show that the proposed approach outperforms competing approaches shown in [10] and [13], by an average of1.4 dB and 0.9 dB, respectively, in terms of the standard PSNR value and by an average of 11.6% and 8.5% in terms of the complex wavelet SSIM index. The enhanced stego-image obtained implies improving the imperceptibility with a comparable embedding capacity compared to thatin [13] and outperforming that in [10] by an average increase of

Table I. PSNR values (in DB), complex wavelet ssim indexes and embedding capacity of the secret bit stream (in bits) using the competing approaches with standard images as cover images.

	The approach in [10]			The approach in [13]			The proposed approach		
Image	PSNR (dB)	CWSSIM index	Capacity (bits)	PSNR (dB)	CWSSIM index	Capacity (bits)	PSNR (dB)	CWSSIM index	Capacity (bits)
Lena	41.09	0.9264	2434603	41.40	0.9334	2437700	42.10	0.9492	2437684
Baboon	34.31	0.7735	2662080	32.76	0.7386	2772545	35.46	0.7995	2772563
Tiffany	39.87	0.8989	2416944	41.98	0.9466	2425193	43.02	0.9699	2425179
Peppers	37.32	0.8414	2435223	38.33	0.8642	2447737	39.27	0.8856	2447740
Jet	40.65	0.9167	2418419	42.51	0.9584	2443492	43.57	0.9823	2443471
Boat	37.14	0.8373	2504613	36.66	0.8265	2539530	38.96	0.8784	2539514
House	38.42	0.8662	2470824	39.19	0.8836	2510373	40.24	0.9072	2510366
Pot	37.51	0.8459	2387494	41.50	0.9356	2394782	42.13	0.9498	2394768

REFERENCES

[1] F.Y.Shih,Digital Watermarking and Steganography:Fundamentals and Techniques. CRC Press, 2017. ISBN978-1498738767

[2] S. Singh and T. J. Siddiqui, Transform Domain Techniques for Image Steganography. LAMBERT Academic Publishing, 2014. ISBN 978- 3659697838G. Bugar, V. Banoci, M. Broda, D. Levický, and D. Dupak, "Data hiding in still images based in blind algorithm of steganography," in the IEEE 24thIntern. Conf. Radioelektronika, April 2014.doi: 10.1109/Radioelek.2014.6828423 pp. 1–4.

[3] S.AhaniandS.Ghaemmaghami,"Colour image steganography method based on sparserepresentation,"IETTrans.onImageProcessing,vol.9, no. 6, pp. 496–505, 2015.doi: 10.1049/iet-ipr.2014.0351

[4] S. Wang, C. Li, and W. Kuo, "Reversible data hiding based ontwodimensional prediction errors," IET Trans. on Image Processing, vol. 7, no.9,p.805U″816,2013.doi:10.1049/iet-ipr.2012.0521

[5] M. A. Dagadit, E. I. Slusanschi, and R. Dobre, "Data hiding using steganography," in the IEEE 12thIntern. Symposium on Parallel and Distributed Computing, 2013. doi: 10.1109/ISPDC.2013.29 pp.159– 166.

[6] T.-C. Lu and Y.-C. Lu, An Improved Data Hiding Method of Five Pixel Pair Differencing and LSB Substitution Hiding Scheme .Springer Intern. Publishing, 2017, pp.67–74.

[7] S. Kumar and S. Muttoo, "Image steganography based on wavelet families," Journal of Computing Engineering Information Technology, vol. 2, no. 2, pp. 1–9, 2013.doi: 10.4172/2324-9307.1000105

[8] S. Gandharba and S. K. Lenka, "A novel steganography technique by mapping words with LSB array," Intern. Journal on Signal Imaging Systems Engineering,vol.8,no.1-2,pp.115-122,2015.doi:10.1504/IJSISE .2015.067052

[9] M. Kalita and T. Tuithung, "A novel steganographic method using 8- neighboring PVD (8nPVD) and LSB substitution," in Intern. Conf. on Systems, Signals and Image Processing, May 2016. doi: 10.1109/IWSSIP.2016.7502756 pp.1–5.

[10] S. Sirsikar and J. Salunkhe, "Analysis of data hiding using digital image signal processing," in the IEEE Intern. Conf. on Electronic Systems, Signal Processing and Computing Technologies,2014.doi:10.1109/ICESC.2014.28 pp.134–139

[11] K.Muhammad,M.Sajjad,I.Mehmood,S.Rho,andS.W. Baik,"Image steganography using uncorrelated color space and its application for security of visual contents in online social networks,"Future Generation Computer Systems.doi:http://dx.doi.org/10.1016/j.future.2016.11.029

[12] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," Multimedia Tools and Applications, vol. 75, no. 21, pp. 13 541–13 556, 2016. doi: 10.1007/s11042-015-2937-2

[13] http://sipi.usc.edu/database/

[14] A. C. Bovik, *The Essential Guide to Image Processing*, 1st ed. Aca- demic Press, 2009. ISBN978-0123744579

[15] Z. Wang and E. P. Simoncelli, "Translation insensitive image similarity in complex wavelet domain," in *IEEE Intern. Conf. on Acoustics, Speech, and Signal Processing*, vol. II, march 2005. doi: 10.1109/ICASSP.2005.1415469 pp.573–576.