

Chaotic Pixel Value Differencing

Nirmala Pun

Computer Science and Engineering UIET, Panjab University, Chandigarh, India
Email: nirmala.pun13@gmail.com

Dr. Mamta Juneja

Computer Science and Engineering UIET, Panjab University, Chandigarh, India
Email: mamtajuneja@pu.ac.in

Abstract—Pixel Value Differencing (PVD) is a spatial steganography technique that is area sensitive and considers complete visual invisibility while data hiding. While Least Significant Bit Approach (LSB) still remains the most popular technique and is simplest in approach its simplicity makes it vulnerable against steganalysis. Our proposed technique is an enhancement over traditional Pixel Value Differencing. We have added a layer of security using chaotic encryption approaches. Also some PVD based hybrid techniques are compared and analyzed to draw conclusions on the basis of various statistical measures.

Index Terms—Pixel Value Differencing, Least Significant Bit (LSB), Chaos, Peak Signal to Noise Ratio, Mean Square Error, Structural Similarity Index Measure.

I. INTRODUCTION

Steganography is the discipline of concealing critical data within innocuous mediums like digital images, audio and video. As superior facilities have emerged in field of capturing, processing and transmitting of digital images, these serve as the most preferred mode of covert communication. Although it is an ancient art its applicability is wide and in combination with more contemporary and compatible techniques like watermarking and encryption, it continues to expand. Before formulating new techniques to obscure data predecessors need to be analyzed and compared so as to weigh in their respective pros and cons. Steganography finds application in several genres but a particular method must be carefully analyzed to check its suitability as per one's own need.

Over the years steganography has tremendously evolved. Two main domains under this area are spatial domain that emphasize on local pixel manipulations and frequency domain which work upon the frequency components of the transform. Our work intends to improve upon a popular spatial steganographic technique viz. Pixel value differencing (PVD). PVD considers the difference between smooth and edge areas and their varied embedding capacity. It tremendously increases the embedding capacity and imperceptibility. As opposed to

LSB it is secure against various statistical and visual attacks thus rendering security. But evolution of newer

attacks has made it vulnerable. So to improve upon secure data transmission message is encrypted using popular encryption algorithms. In our proposed approach Chaotic PVD(C-PVD), we use chaotic encryption to secure the payload. The use of chaos for encryption is a relatively new technique. When applied to traditional steganography it generates visually imperceptible carrier images. Also even if the presence is detected, such arrangement makes it difficult for the attacker to reconstruct the original message.

Remainder of the paper is organized as follows: section II comprises of related works in this particular domain, brief background and observations of the review process. Section III describes the proposed approach and work flow. The conclusions drawn are presented in section IV. Section V contains acknowledgment and section VI includes references.

II. RELATED WORK

Pixel Value Differencing (PVD) method [1] proposed by Wu and Tsai ensures selective embedding in smooth areas and edges to hide different quantities of secret data. The entire pixel range was divided into multiple sub ranges. The cover image was raster scanned and then divided into blocks of two non overlapping pixels. A difference value was calculated from each such block to modify the original pixel values. This modification was performed such that the pixel ranges never go out of range.

Let us assume p_i and p_{i+1} are two pixels of the considered block then difference d is given by $(p_{i+1}-p_i)$. Suppose it lies in the sub range r_1 with width w_1 , then number of bits to be embedded t can be calculated by $\log_2(w_1)$. The decimal value of t bits of secret data is taken and used to adjust d to get d' . This d' gives us new values p_i' and p_{i+1}' of pixels p_i and p_{i+1} . The embedding is explained using a block of [50,200] in figure 1 below:

PVD method has been subsequently improved in further works and combined with various other popular methods to achieve more capacity, security, robustness and imperceptibility.

Wu et al. [2] proposed a modified PVD approach. The partitioning and difference calculation steps were on the same lines as original PVD. Users controlled the division of range table into lower division (smooth regions) or

higher division (edge regions) .This division was used as a key for the extraction of secret message from stego image. If the pixel difference of a block was under higher level then original PVD was used for embedding otherwise 3 bit LSB substitution was employed. Improved image quality was achieved using this method.

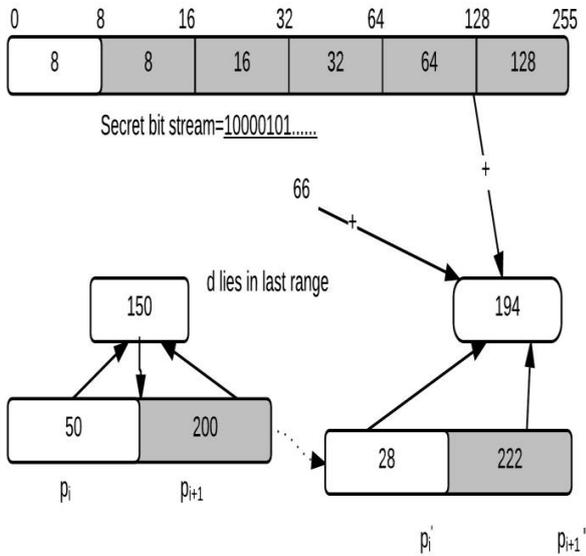


Fig.1. PVD embedding Process

Yang et al. [3] proposed a modified k-bit LSB substitution method in which k was decided by the range in which the block difference fell. In this approach two dividing cases were considered: lower and higher (l-h) division and lower, middle and higher (l-m-h) division. The embedding capacity increased in this particular order i.e. from l to h. After the difference was calculated for a block, range was checked and as per that either l or m or h bits of secret data was hidden. A readjustment phase was executed if the difference values changed after embedding. Experiments carried out with different divisions of l-h and l-m-h confirmed better results in terms of adaptability, capacity, and imperceptivity as compared to Wu et al.'s [2] method.

Wang et al. [4] proposed modulus PVD method in which embedding was done using the modulus function. The difference of the two pixel block was used to modify the pixel values by employing the modulus operation. On comparing with Wu Tsai method this yielded similar values of capacity and with higher PSNR. It tackled the falling off problem by adjusting the remainders of pixel block. This method has also been tested secure against RS detection attack.

Ko-Chin Chang et al. [5] proposed a direction sensitive PVD approach (TPVD).This method used three pixel pairs in a 2x2 block. Two horizontal and one diagonal pixel pairs were utilized. For choosing the reference point and minimize image distortion, an optimal rule accompanied with adaptive rules was presented. It provided more imperceptible stego image as compared to original PVD. Also it was secure against dual statistics attack.

Weiqi Luo et al. [6] proposed a secure content adaptive PVD scheme. In this method, cover image was partitioned into small squares and rotated by any random degree of 0, 90, 180 or 270. The resulting image was then divided into non-overlapping embedding units with three consecutive pixels, and the middle one was used for embedding. The number of embedded bits was dependent on the differences among the three pixels. In order to preserve the local statistical features, the sort order of the three pixel values was kept same after data hiding. Furthermore, the new method first used sharper edge regions for hiding adaptively, while preserving other smoother regions by adjusting a parameter. The experimental results evaluated on a large image database showed that this method achieved much better security as compared to the previous PVD-based methods.

Medeni et al. [7] proposed a four pixel differencing method with LSB substitution. In this the cover was partitioned into equal blocks of 4x4. After that, for each block M i.e. square root of median was calculated. Then average difference D was calculated. If $D \geq M$, embedding was performed as per MSB's. Each pixel was divided into two parts. MSB was checked for number of 1's. For 4 or 3 1's 'b' bits could be embedded in LSB. For two 1's 2bits could be embedded. For zero or one 1's single bit would be hidden in one LSB. Thus it adaptively decided the number of secret data to be hidden. Also k-bit LSB substitution was used to hide the bits. This method was compared with PVD and established better values of PSNR and greater embedding performance.

Manjunath et al. [8] proposed an improved modulus PVD and further clubbed it with LSB replacement. Using only modulus PVD the entire hiding capacity was underutilized. But when used in combination with LSB replacement, its data hiding capacity improved tremendously. Here based on a threshold to determine whether a pixel fell in either smooth area or edge area, LSB method was used otherwise modulus PVD was used. Thus embedding for smooth areas was done using LSB replacement and modulus PVD was used for embedding data in edges. This method was compared with modulus PVD in terms of hiding capacity. It provided greater values of PSNR and improved embedding capacity.

Liao et al. [9] proposed a four pixel differencing approach which also used k bit LSB substitution. In this the cover was partitioned into blocks of 4 pixels. Then average difference was calculated using the minimum pixel and rest of the three pixels. This difference was used to determine the range i.e. higher or lower which in turn gave the number of bits k to be embedded. k was used for k bit substitution in the 4 pixels. Subsequently a readjustment step was applied to extract the secret data.

Khodaei et al. [10] proposed an adaptive approach using LSB and PVD. In this method the range was divided into lower range and higher range, each one further having sub-ranges among them. The cover was partitioned into equal blocks of 3 consecutive bits. The middle pixel was taken as base pixel and its k LSB's were replaced by k bits of secret data. The difference value was used to adjust value of base pixel. Also, two difference

values were obtained from 1st and 3rd pixels and new base pixel. Then the sub ranges of these differences were checked. Data was inserted in base pixel using k bit LSB substitution. While PVD was used to embed data into the 1st and 3rd pixels. The said method when compared with techniques of Wu et al.[2], Yang et al.[3] and Lee et al.[23] yielded greater embedding capacity and imperceptible stego image with acceptable values of PSNR. Also this method has low time complexity.

Mandal et al. [11] proposed a PVD method for color images. In this method, the image was decomposed into its three color component matrix. After that each component was used to embed different number of secret bits. Starting from red component, difference for first block was computed, then for green and then for blue. Same sequence went on for second block and so on. For each block, difference was calculated and respective range was determined. This gave the number of secret bits to embed. For each color block there was a set bit limit. The overflow problem was tackled by applying a checking mechanism on the MSB. If range exceeded, MSB of secret bit stream was discarded before it could have been embedded. If again it went beyond range, then value was embedded in a single bit rather than both the bits of the block. The said method has been compared with PVD; it has achieved better stego image quality, security and PSNR in case of color image. However the results were almost similar when gray images were tested.

Weng et al. [12] proposed a method based on predictive differencing. In this method, the cover image was scanned in a raster scanned manner. Then using various predictors like horizontal, vertical, PV was calculated. Predictive error was computed as a difference of PV and input pixel. The range in which this lied was checked then embedding was done using k bit substitution. If after embedding PE and NPE were laying in different ranges the output pixel's value had to be readjusted. This method has been compared with earlier works of Chang and Tseng's two-side-match, Wu and Tsai's pixel-value differencing, Hang et al.'s spatial domain hiding scheme. Comparatively this method has achieved better capacity and stego image quality.

Mahjabin et al. [13] proposed a block based method using PVD and LSB substitution. In this the image was partitioned into group of 16 pixels, each such pixel group was further divided into two, 8 pixel blocks. For each block its type was determined i.e. vertical or horizontal using the smallest pixel value. If value was odd, block has to be traversed vertically otherwise traversing was horizontal. In each block differences were calculated using the other seven bits and the smallest pixels and these values helped to determine the embedding capacity as per range table. Doing so, the bits to embed for both blocks were combined. This work was implemented as a dynamic data hiding method based on modified PVD and 3 bit LSB. A threshold of 21 bits per block to embed was fixed. If number of bits to hide was greater than 21, LSB substitution was used to hide data otherwise PVD was employed. This work when compared to 3 bit substitution

and two other recent methods yielded better PSNR and embedding capacity.

Sabokdast et al. [14] proposed a method using modified LSB (MLSB) and modulus function with pixel value differencing (MF&PVD) techniques. Instead of simple pixel differencing modulus PVD was roped in to reduce distortions rising due to embedding process. For higher range, modulus PVD was used to hide data. Otherwise modified LSB was used. The secret bits were embedded such that some bits of it were hidden in 1st pixel of block and some were hidden in the 2nd pixel of the block. This resulted in new pixel values of a block. The new and old pixel values of 1st pixel of block were subtracted and as per this difference bits were changed either from 0 to 1 or 1 to 0. Proposed method was compared with methods[1],[2] and[4]. Experiments proved that proposed method has higher PSNR and embedding capacity as compared to all these methods.

Swain [15] proposed a steganographic technique with nine pixel differencing and modified LSB substitution. The image was partitioned into 3×3 pixel blocks and average difference was calculated using minimum value pixel. This difference could belong to any of the 4 levels viz. lower, lower- middle, higher-middle and higher for which n bit(n=2,3,4,5 respectively) LSB substitution was used. Also two LSB's of last pixel in the block were reserved as indicator for data extraction. Comparisons were drawn in terms of PSNR, MSE, embedding capacity and distortion rate between proposed method and Wu et al.'s[2] method. Proposed method has significantly improved results in most cases.

Gulve et al. [16] proposed a PVD method utilizing 5 pixel blocks and LSB substitution. An average value is calculated and the pixel block is modified using the average value of the number of bits that can be embedded in the block. In this a common pixel is used to hide 3 bits of secret data. The proposed method yields better PSNR values in the range of 40 db. The original image is not required to regenerate the message. This method demonstrates imperceptible stego image even after full capacity embedding. Further in [17] they proposed to use PVD for embedding data into the frequency coefficients, thereby performing cross between spatial and frequency domains. It improved upon the robustness of basic PVD with acceptable levels of embedding and imperceptibility.

Hayat et al. [18] proposed a stenographic technique for inserting patient's data in biomedical images. A region of non interest (RONI) was separated and used to hide data using PVD. As in PVD, blocks were divided but only some were used for embedding. Selection of blocks was based on the threshold value. For secure embedding (7, 4) hamming code was used i.e. 3 secret bits have been hidden in 4 cover bits. The said method have been evaluated using MRI and Ultrasound images as cover at varied levels of threshold values and provided improved payload capacity and achieved PSNR more than 50dB.

El-Sayed et al. [19] proposed a modified PVD technique which is secured using logistic chaotic maps. It emphasizes on the security factor by defeating the

histogram attack. Also additional security layer is added to make the extraction by unauthorized person more difficult. Here the image is divided into 2×2 block after a zigzag scan. Hereafter the blocks are rotated in either left or right direction. Two parameters: initial condition and control parameter act as the secret keys and provide for enhanced security. The proposed method is compared with Wu Tsai's original PVD and it performs better in terms of PSNR and embedding capacity. Also added security against histogram analysis makes comparatively superior. The said method is tested on gray images.

R. L. Tataru et al. [20] proposed an adaptive least-significant bit (LSB) approach clubbed with chaotic ordering and pixel-value differencing (PVD). This was an improvement over Yang et al's method which used modified LSB insertion and PVD to hide data in gray scale images. A chaotic generator was used to assist random embedding in the cover and spread the secret data across the entire region. Yang et al's method has been modified using a chaotic generator.

Zagbani et al. [21] proposed a technique in which data was spread out throughout the entire cover using logistic map. It emphasized on encrypting data before inserting into cover for added security. Embedding was done on the basis of adjacent pixels relation.

A. Background

PVD betters the traditional LSB approach by selective embedding of data. It works on differences of adjacent pixels and modifying their values according to differences ranges. It explores different regions of image and hides data accordingly. The techniques compared in this paper are extensions of traditional PVD approach and also makes use of LSB. Additionally grayscale and color PVD are considered separately.

B. Quality Parameters

The pre and post versions of image are compared on the basis of achieved and desired imperceptibility, robustness and security.

The most widely used parameters are explained below

Mean Square Error (MSE) [22]

It the most common estimation method used to check image fidelity. It takes into account full reference model. It is widely used as it is simple to implement and cheaper in execution. Let us consider two images, $x(i, j)$ and $y(i, j)$ of $M \times N$ dimensions. The MSE is calculated as

$$MSE = \frac{1}{MN} \sum_{i=0}^M \sum_{j=0}^N (x(i, j) - y(i, j))^2 \quad (1)$$

Peak Signal to Noise Ratio (PSNR) [22]

PSNR employs MSE to evaluate image quality and is inversely related to it. It is expressed as the ratio of original image against corrupted image and is measured in terms of logarithmic decibel (dB). Our aim is to achieve higher values of PSNR. Higher values indicate better reconstruction. These do not take into consideration the human visual system. It is calculated as

$$PSNR = 10 \log_{10} \left(\frac{2^n - 1}{\sqrt{MSE}} \right) = 10 \log_{10} \left(\frac{255^2}{\sqrt{MSE}} \right). \quad (2)$$

Embedding capacity

The amount of data that can be inserted in a cover image while maintaining the statistical properties, determines the embedding capacity. Different methods provide different levels of capacity. Also the payload is directly proportional to size of cover image. Generally, if the host image has more smooth regions then lesser data may be hidden. On the other hand, complex images having frequent edge variations which provide comparatively greater insertion capacity. This is generally measured in bits per pixel (BPP).

$$capacity = \frac{N_{bits}}{C} \quad (3)$$

N_{bits} is the number of secret data bits and C is the cover image bits.

Structural Similarity Index Measure (SSIM)[22]

In addition to these traditional parameters a newer quality measure called Structural Similarity Index Measure (SSIM) is being used to ensure imperceptibility.

$$SSIM = \frac{(\overline{2 \times x \times y} + C1) \times (\overline{2 \times \sigma_{xy}} + C2)}{(\overline{\sigma_x^2 + \sigma_y^2} + C2) \times ((\overline{x})^2 + (\overline{y})^2 + C1)} \quad (4)$$

Where x and y are local windows of same size. $C1$ and $C2$ are empirically chosen positive constants, \bar{x} and \bar{y} are (respectively) means of x and y , σ_x and σ_y are (respectively) standard deviations of x and y , σ_{xy} is the cross correlation of x and y . SIM produces decimal values in the range of $(-1, 1)$.

Table 1. Summary of various techniques

Technique	Cover image	Embedding capacity (bites)	PSNR(db)	Attacks/Comments
For Grayscale Images				
PVD [1]	Lena	409752	38.94	Dual statistics attacks
	Baboon	457168	33.43	
	Peppers	407256	37.07	
PVD+LSB replacement [2]	Lena	766040	36.16	RS Steganalysis
	baboon	717848	32.63	
	peppers	770248	35.34	
Adaptive edge PVD [3]	Lena	807256- 812794	37.93-41.39	Not tested
	Baboon	854096 -874642	34.84-38.58	
	Peppers	800168-804266	38.78-42.42	
PVD and Modulus function [4]	Lena	409752	44.1	RS Steganalysis
	Baboon	457168	40.3	
	Peppers	407256	43.3	
TPVD [5]	Lena	606688	38.89	RS Steganalysis
	Baboon	659256	33.93	
	Peppers	604632	38.50	
	Baboon	659256	33.93	
	Peppers	604632	38.50	
4PVD+modified LSB [9]	Lena	578716- 1070440	33.66-44.31	Trade off between embedding capacity and attack resistance
	Baboon	701580- 1116068	32.02-41.76	
	Peppers	569512 -1062232	34.06-44.58	
New Adaptive PVD [10]	Lena	809 966	37.63	RS steganalysis Spam features
	Baboon	886 516	36.29	
	Peppers	802 228	37.97	
Predictive differencing PVD [12]	Lena	798478-821121	34.573-36.786	Not presented
	Baboon	946068-878413	29.128-32.755	
	Peppers	796092-811227	33.910-36.153	
Modulus+modified LSB [14]	Lena	66064- 95748	40.23-43.77	Not tested
	Baboon	66397-91914	39.79-42.38	
	Peppers	65889-95403	40.04- 43.11	
For Colour Images				
Colour PVD [11]	Lena	1166296	42.26	Not tested
	Baboon	1159328	38.44	
	Peppers	1167960	42.28	
9PVD [15]	Lena	2297680	40.64	RS steganalysis
	Baboon	2877658	35.22	
	Peppers	2286574	39.52	

In this paper we compare a range of hybrid PVD techniques by using three widely used cover images viz.

Lena, baboon and peppers each having size 512×512. The comparisons have been drawn by conducting tests on gray scale images. PSNR and embedding capacity have been complied. Some of the considered methods have been tested against attacks and security analyses which have been discussed whereas some methods remain untested. Chi square attack, RS steganalysis, histogram analysis are the most popular steganalysis attacks.

We observe from the above drawn comparisons that as the method flourished with time, more and more data

capacity became available. In comparison to simple PVD [1] the capacity has nearly doubled in subsequent techniques. Also these new methods improved the image quality and yield better statistical results be it PSNR or MSE. This means a stego image is quite similar to original image. Methods in latter times extended over colour images in addition to grayscale images. We observe that colour PVD methods [11], [15] yield very high capacity against their grayscale counterparts. Also most of the methods have been tested against only one or two attacks like RS attacks. For new steganalysis threats it is very vulnerable

III. PROPOSED APPROACH

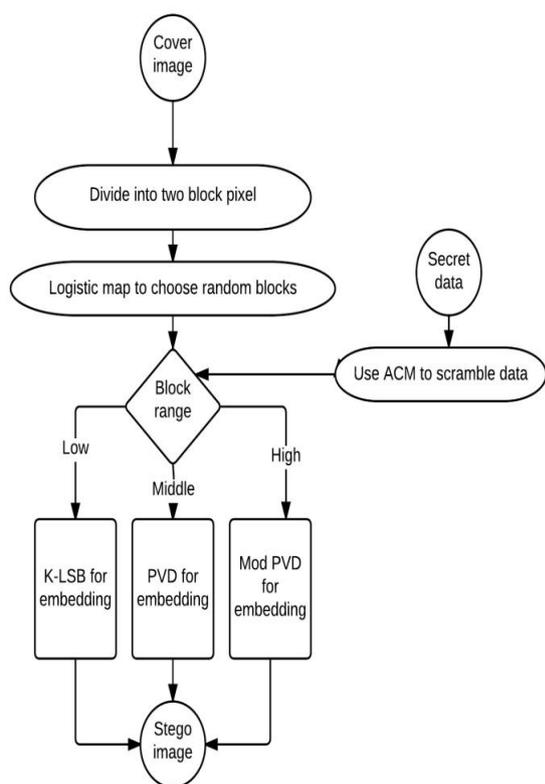


Fig.2. The Proposed Approach

We are using a data-set of standard image processing images. Tests are run on 512×512 image size. The range table of [0,255] is divided into range widths of 8, 8, 16, 32, 64, and 128; thus the total range is partitioned into [0, 7], [8, 15], [16, 31], [32, 63], [64,127] and [128,255].

We employ the principles of chaos in order to enhance the security of PVD approach. 1 D logistic map proposed by R.M. May is one of the simplest chaotic systems [23].

$$x_{k+1} = \mu x_k (1 - x_k) \quad (5)$$

Where $0 \leq \mu \leq 4$ and when $3.5699456 < \mu \leq 4$, the map is in the chaotic state.

Meanwhile chaotic sequence is of the utmost sensitivity for the initial value, and is very precise on the key requirements while extracting secret message, thus it can ensure the secrecy of information security effectively.

Another chaotic map used in our approach is the 2D Arnold Cat Map (ACM). It is an area preserving map and after a number of iterations the image returns to its initial state. Mathematically it is represented as [23]:

$$x' = (x + ay) \bmod(N) \quad (6)$$

$$y' = (bx + (ab + 1)y) \bmod(N) \quad (7)$$

Where, a, b are control parameters which are positive integers and (x', y') is the new position of the original pixel position (x, y) of $N \times N$ plain-image when Cat map is applied once to the original.

Our algorithm proceeds in following manner:

1. The cover image is scanned in a zigzag manner starting from the extreme left.
2. Then the image is divided into two pixel blocks.
3. The blocks are shuffled using 1D Logistic map.
4. ACM is used to scramble the secret image.
5. Then difference is calculated depending upon which the embedding process is carried out.
6. The entire range is divided into three sub ranges viz. low, middle and high.
7. The low range consists of difference values less than 8 and performs LSB embedding.
8. The middle range consists of values between 8 and 64 and uses PVD to perform embedding.
9. The high range consisting of values from 65 to 255 uses modulus PVD to perform embedding.
10. Combining these three approaches gives better results in terms of PSNR and SSIM.

Our work also includes the comparison of 2 LSB, PVD and modulus PVD with our method C-PVD. The matrices for comparison are embedding capacity in bits, MSE and PSNR. Also we compare the techniques to check structural similarity using SSIM.

IV. CONCLUSION

Despite a number of techniques being developed in this area, different methods provide application in specific fields. A comparative analysis provides the clear picture of what all a particular method can achieve. And further for what purpose it can be used. Primarily, embedding capacity is the prime concern when developing any new algorithm. There is generally a tradeoff between security and capacity. And for higher capacity, security is compromised. Security is generally implemented by adding an additional layer of encryption. If security concerns are at stake then encryption is clubbed with Steganography.

Our approach achieves a higher embedding capacity and is secure against attacks. Also it yields higher values of SSIM thereby providing better imperceptibility.

ACKNOWLEDGEMENT

We express our sincerest gratitude towards every individual involved with this work. The researchers and academicians whose valuable endeavors in this field have provided the basis for our work are deeply appreciated.

REFERENCES

[1] Da-Chun Wu and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", *Pattern*

- Recognition Letters*, Vol.24, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.
- [2] 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,doi:10.1049/ip-vis:20059022.
- [3] Cheng-Hsing Yang, Chi-Yao Weng, Shih-Jeng Wang and Hung-Min Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems”, *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3,2008,doi: 10.1109/TIFS.2008.926097.
- [4] C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, “A high quality steganographic method with pixel-value differencing and modulus function”, *The journal of system and software*, Vol. 81, pp. 150-158,2008, doi:10.1016/j.jss.2007.01.049.
- [5] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu, “A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing”, *Journal of Multimedia*, Vol. 3, No. 2, 2008, doi:10.4304/jmm.3.2.37-44.
- [6] Weiqi Luo, Fangjun Huang and Jiwu Huang, “A more secure steganography based on adaptive pixel-value differencing scheme”, *Springer Science+Business Media, LLC* 2009, doi: 10.1007/s11042-009-0440-3.
- [7] M.B. Ould Medeni and El Mamoun Souidi, “A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution”, *International Conference on Multimedia Computing and Systems (ICMCS) IEEE*, 2010, doi:10.1109/ICMCS.2011.5945688
- [8] Manjunath Gadiparthi, Keshav Sagar, Divya Sahukar and Rakesh Chowdary, “A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods”, *International Journal of Computer Applications*, Vol. 22, No.5, 2011,doi: 10.5120/2582-3568.
- [9] Xin Liao, Qiao-yan Wen and Jie Zhang, “A steganographic method for digital images with four-pixel differencing and modified LSB substitution”, *Journal of Visual Communication and Image Representation*, Vol. 22, Iss. 1, pp. 1–8, 2011,doi:10.1016/j.jvcir.2010.08.007.
- [10] M. Khodaei and K. Faez, “New adaptive steganographic method using least significant-bit substitution and pixel-value differencing”, *IET Image Process*, Vol. 6, Iss. 6, pp. 677–686, 2012, doi:10.1049/iet-ipr.2011.0059.
- [11] J. K. Mandal and Debashis Das, “Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain”, *International Journal of Information Sciences and Techniques (IJIST)*, Vol.2, No.4, 2012,doi : 10.5121/ijist.2012.2408 .
- [12] C.Y. Weng, H.K. Tso and S.J. Wang, “Steganographic data hiding in image processing using predictive differencing”, *Opto-Electronics Review*, Vol. 2, Iss. 2, pp. 126-133, 2012, doi: 10.2478/s11772-012-0020-3.
- [13] Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque, “A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method” *5th International Conference Computer and Information Technology (ICCIIT)*, 2012, doi: 10.1109/ICCIITechn.2012.6509770.
- [14] Masume Sabokdast and Majid Mohammadi, “A Steganographic Method for Images with Modulus Function and Modified LSB Replacement Based on PVD”, *5th Conference on Information and Knowledge Technology (IKT) IEEE*, 2013, doi: 10.1109/IKT.2013.6620050.
- [15] Gandharba Swain, “ Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution”, *Indian Journal of Science and Technology*, Vol. 7(9),pp. 1448–1454, 2014,doi: 10.17485/ijst/2014/v7i9/49029.
- [16] Avinash K. Gulve and Madhuri S. Joshi, “A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution”, *International Journal of Image, Graphics and Signal Processing*, 2015, doi: 10.5815/ijgsp.2015.05.08 .
- [17] Avinash K. Gulve and Madhuri S. Joshi, “An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach”, *Mathematical Problems in Engineering*,Vol.2015,doi:10.1155/2015/684824
- [18] Hayat Al-Dmour, Ahmed Al-Ani and Hung Nguyen, “An Efficient Steganography Method for Hiding Patient Confidential Information”, *36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'14)*, 2014, doi: 10.1109/EMBC.2014.6943569.
- [19] El-Sayed M. El-Alfy and Azzat A. Al-Sadi, “Improved Pixel Value Differencing Steganography Using Logistic Chaotic Map”, *International Conference on Innovations in Information Technology (IIT)*, 2012,doi: 10.1109/INNOVATIONS.2012.6207716.
- [20] R. L. Tataru, D. Battikh, S. El Assad and H. Noura O. Deforges, “Enhanced Adaptive Data Hiding in Spatial LSB Domain by using Chaotic Sequences”, *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2012,doi:10.1109/IIH-MSP.2012.26.
- [21] Soumaya Zaghbani and Rhouma Rhouma, “Data Hiding in Spatial Domain Image Using Chaotic Map”, *5th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO) IEEE*, 2013, doi: 10.1109/ICMSAO.2013.6552626.
- [22] Alain Horé and Djemel Ziou, “Image quality metrics: PSNR vs. SSIM”, *International Conference on Pattern Recognition*, 2010, doi:10.1109/ICPR.2010.579.
- [23] Musheer Ahmad and M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, *International Journal on Computer Science and Engineering*, Vol. 2 (1), 46-50, 2009, doi: 10.1.1.208.6906.

Authors' Profiles



Nirmala Pun is pursuing her M.E. in Computer Science and Engineering from UIET Panjab University Chandigarh. Her research area is steganography and information hiding



Dr. Mamta Juneja is an assistant professor in UIET Panjab University Chandigarh. She has numerous publications in various international journals, international and national conferences. She is a reviewer for several national and international journals and conferences. Her areas of interest are image processing, biometrics, information security and hiding.