I J C T A, 9(20), 2016, pp. 337-345

A hybrid approach in spatial domain for image steganography

Nirmala Pun* and Mamta Juneja**

ABSTRACT

Spatial steganography is a popular genre of data hiding. It provides features like large embedding capacity and simplicity in application. In this paper we propose a hybrid spatial steganography method based on pixel value differencing (PVD) for safe data transmission. In this approach we perform random embedding of secret data such that we use PVD for smooth regions and modulus PVD for edged regions respectively. Also we use chaotic encryption to render more security to the method. Experimental results quantitatively establish that the proposed technique provides imperceptibility and robustness to the embedded data.

Keywords: Chaos, data hiding, peak signal to noise ratio (PSNR), pixel value differencing (PVD), steganography.

1. INTRODUCTION

Steganography [1] is a field of information hiding dealing with covert communication. There are many algorithms available for secure transmission of data over unsecure media. When digital images are used as the vessels of communication then there are broadly two genres of hiding data. These are spatial domain and frequency domain. Both have their own pros and cons. As far as spatial techniques are concerned these have high embedding capacity and thus can have more secret data embedded in particular region without visible distortion. Also these are easier in implementation and render less complexity while implementation. In frequency domain work is concentrated upon the transforms of the images. These pose great complexity but are very secure. The choice of a specific algorithm depends on the type of hardware, software and the ultimate application destined. The three parameters for choosing any suitable algorithm are imperceptibility, robustness and capacity. So there is always are tradeoff among these qualities.

Pixel value differencing (PVD) [2] is a spatial domain method of steganography. It is very popular and has been improved upon over years of research. The strengths have been multiplied and the limitations have been overcome to a great extent. PVD is a successor to LSB method with comparable embedding capacity and can withstand the attacks performed upon it.PVD has different versions and have been amalgamated with popular techniques of other genres like cryptography, watermarking, fuzzy networks to render more versatility. PVD's most exhausted work is in combination with LSB [3] [4][5][6]. PVD as a technique has also been experimented with. Further for increasing robustness encryption was performed over secret data and then steganography was performed. Initially classical encryption approaches like RSA, DES [7] [8] were employed but later other encryption genres were discovered and applied. One such domain is chaotic encryption. Chaotic encryption has basis in chaos theory which is characterized by Ergodicity, sensitivity to initial parameters and random behavior of deterministic nature. Due to such properties chaotic techniques have appealing applications in secure data communication. Popular chaotic maps in application are Logistic maps, Arnold Cat map, tent map, Heron map and Baker map. These have applicability in different dimension and being simpler in implementation one and two dimensional versions are very popular.

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

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

El Sayed [9] devised secure modified PVD using secure logistic maps thus providing an extra layer of protection against attackers. It also withstood the histogram attack thus augmenting the security factor. Tataru et al. [10] clubbed LSB with chaotic ordering and PVD. In this they use a chaotic generator for churning sequences for randomly spreading the data over the entire image.

In our work we consider two versions of PVD for data embedding. Rather than working the image as a whole we partition the entire image into two regions viz. smooth areas which have little difference in pixel values and intensities and edge areas which constitute for vast differences into pixel intensities and values. For additional security we add the techniques of chaotic encryption during the embedding process so that even if the imperceptibility is Ease of Use compromised then also the integrity of secret data is not compromised. In chaotic encryption maps are used for introducing confusion and diffusion. We use two very popular maps for securing our steganographic algorithm .1 D logistic map is used as pseudorandom generator. It is a very sensitive sequence generator and depends on initial values of parameters. Even a slight variation in values can result in a whole other series. Here we use it for selecting random blocks for embedding as sequential embedding is very mundane and easy to crack. Also for rendering additional protection to the sensitive secret data we use two dimensional Arnold's cat map (2D ACM) for scrambling it. So the security factor is introduced at every level of steganographic process.

1.1. Related works

In PVD [2] the cover image is scanned in a crisscross order starting from the upper left corner and subsequently divided it into two pixels blocks of non over lapping pixels. The difference obtained from these pixel blocks are used to carry out the alteration of the existing pixels into new pixel block. The range of gray pixel value spans from 0 to 255. Wu and Tsai experimented using several pixel sub ranges. The entire gray range had two set of widths. The range widths 8, 8, 16, 32, 64, and 128, partitioned the full range into [0 7]; [8 15]; [16 31]; [32 63]; [64 127] and [128 255]. The second set had range widths of 2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, and 64.A word formatted file was used as message in this process. For an image C of size $m \times n$ a raster scan is performed to generate sub images C_i such that $C= \{C_i | i=1, 2, 3\ldots. (m \times n)/2\}$. Each individual block C_i will have two pixels having values $p_{(i,x)}$ and $p_{(i,y)}$. The difference such obtained is

$$d_i = | p_{(i,x)} - p_{(i,y)} |. \tag{1}$$

The range table was intended for providing embedding capacity of each C_i. The entire range R is partitioned into k contiguous sub ranges. Each sub range R_k has a lower bound l_k and upper bound u_k. The width w_k of a particular C_i is computed by

$$w_k = u_k - l_k + 1. \tag{2}$$

The amount of secret data to be embedded is determined by t_i=floor (lg (w_k)). t'_i is the decimal equivalent of t_i. d'_i is the modified value of d_i.

$$d'_i = t'_i + l_k \tag{3}$$

Next the secret data is implanted into C_i by modifying pixels as follows:

$$p'_{(i,x)}, p'_{(i,y)} = \begin{cases} 1. & p_{(i,x)}+\text{ceil}(\text{diff}/2), p_{(i,y)}-\text{floor}(\text{diff}/2); \\ & \text{if } p_{(i,x)} \geq p_{(i,y)} \text{ and } d'_i > d_i \\ 2. & p_{(i,x)}-\text{floor}(\text{diff}/2), p_{(i,y)}+\text{ceil}(\text{diff}/2); \\ & \text{if } p_{(i,x)} < p_{(i,y)} \text{and } d'_i > d_i \\ 3. & p_{(i,x)}-\text{ceil}(\text{diff}/2), p_{(i,y)}+\text{floor}(\text{diff}/2); \\ & \text{if } p_{(i,x)} \geq p_{(i,y)} \text{ and } d'_i \leq d_i \\ 4. & p_{(i,x)}+\text{ceil}(\text{diff}/2), p_{(i,y)}-\text{floor}(\text{diff}/2); \\ & \text{if } p_{(i,x)} < p_{(i,y)} \text{ and } d'_i \leq d_i \end{cases} \tag{4}$$

Here diff = $|d'_i - d_i|$. So the embedding is performed by replacing new values of $p_{(i,x)}$, $p_{(i,y)}$ in cover image C.

Modulus PVD [11] additionally utilizes the remainder computed using modulus function to modify the pixel values. Also it yielded better stego image quality as compared to original PVD. This method alters the pixel values by calculating remainder value in the following manner:

$$P\_rem_i = (p_{(i,x)} + p_{(i,y)}) \bmod t'_i \tag{5}$$

$$diff = |P\_rem_i - t'_i|.$$

$$diff1 = 2^{ti} - |P\_rem_i - t'_i| \tag{6}$$

The pixel values are changed using following:

$$p'_{(i,x)}, p'_{(i,y)} = \begin{cases} 1. & p_{(i,x)} - ceil(diff/2), p_{(i,y)} - floor(diff/2); \\ & \text{if } P\_rem_i > t'_i \text{ and } diff \le 2^{ti}/2 \text{ and } p_{(i,x)} \ge p_{(i,y)} \\ 2. & p_{(i,x)} - floor(diff/2), p_{(i,y)} - ceil(diff/2); \\ & \text{if } P\_rem_i > t'_i \text{ and } diff \le 2^{ti}/2 \text{ and } p_{(i,x)} < p_{(i,y)} \\ 3. & p_{(i,x)} + floor(diff/2), p_{(i,y)} + ceil(diff//2); \\ & \text{if } P\_rem_i > t'_i \text{ and } diff > 2^{ti}/2 \text{and } p_{(i,x)} \ge p_{(i,y)} \\ 4. & p_{(i,x)} + ceil(diff/2), p_{(i,y)} + floor(diff/2); \\ & \text{if } P\_rem_i > t'_I \text{ and } diff > 2^{ti}/2 \text{ and } p_{(i,x)} < p_{(i,y)} \\ 5. & p_{(i,x)} + floor(diff/2), p_{(i,y)} + ceil(diff/2); \\ & \text{if } P\_rem_i \text{ d" } t'_i \text{ and } diff \le 2^{ti}/2 \text{and } p_{(i,x)} \ge p_{(i,y)} \\ 6. & p_{(i,x)} + ceil(diff/2), p_{(i,y)} + floor(diff/2); \\ & \text{if } P\_rem_i \le t'_i \text{ and } diff \le 2^{ti}/2 \text{and } p_{(i,x)} < p_{(i,y)} \\ 7. & p_{(i,x)} - ceil(diff1/2), p_{(i,y)} - floor(diff1/2); \\ & \text{if } P\_rem_i \le t'_i \text{ and } diff > 2^{ti}/2 \text{and } p_{(i,x)} \ge p_{(i,y)} \\ 8. & p_{(i,x)} - floor(diff1/2), p_{(i,y)} - ceil(diff1/2); \\ & \text{if } P\_rem_i \le t'_i \text{and } diff > 2^{t}/2 \text{ and } p_{(i,x)} < p_{(i,y)} \end{cases} \tag{7}$$

The overflow problem is handled by adding three additional steps after the readjustment of original pixels to obtain values $p'_{(i,x)}$ and $p'_{(i,y)}$.

2.1. Arnold's Cat Map (ACM)

Another widely used chaotic map is the Arnold Cat Map [12], which alters of the pixel values positions. Arnold cat map demonstrates the phenomenon of generating order from an apparent random system .When hit with a transformation, the pixels of an image show random disorder but if such image is iterated some fixed number of times, the original image just reappears.

This map uses three keys for image encoding viz. two parameters p, q and m, the number of iterations.

For a matrix $X = \begin{bmatrix} x \\ y \end{bmatrix}$, the ACM is mathematically represented as the following,

$$\Gamma : \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

The parameters p and q are bound under certain criterions which are stated as:

- Both must be integral values
- Determinant of $\left(\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\right)$ must be equal to 1, therefore preserving the area and keeping the image size same which will keep the size of the image the same all through the subsequent iterations.

The above mentioned system may also be represented as,

$$a_{n+1} = (2a_n + a_n) \bmod 1$$
$$b_{n+1} = (b_n + y_n) \bmod 1 \quad (8)$$

2.2. Logistic map

The one-dimensional Logistic map is proposed by R. M. May [13] is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behavior.

$$L_{k+1} = \mu\, L_k (1-L_k) \quad (9)$$

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

The sequences generated by the logistic map are very sensitive to initial conditions, in the sense that two logistic sequences generated from different initial conditions are uncorrelated statistically. Moreover, all the orbits of the logistic map are dense in the range of the map [0, 1].

2. PROPOSED ALGORITHM

The proposed approach is a modification over the simple PVD. It has been strengthened using chaotic encryption. We proceed by scanning and dividing the cover image into blocks then we chose a random block based on the sequence generated by the logistic map. As per the value of difference either PVD or mod PVD is employed. Also the secret image is scrambled using the ACM and converted into a binary data stream for embedding. Each block is approached for embedding till the data finishes or all the blocks get used up. In Fig. 1 the grayscale range division is shown.

2.1. The embedding algorithm

Figure 2 shows the block diagram of embedding algorithm. Here we have assumed two divisions "High" and "Low". As shown in fig. 2, the low division has R1 and R2 levels whereas high division has levels R3, R4, R5 and R6.

The data embedding takes place in following manner.

Step 1: Calculate the difference diffi for each two pixel block $[p_{(i,x)}\ p_{(i,y)}.]$

$$diffi = | p_{(i,x)} - p_{(i,y)}. |$$

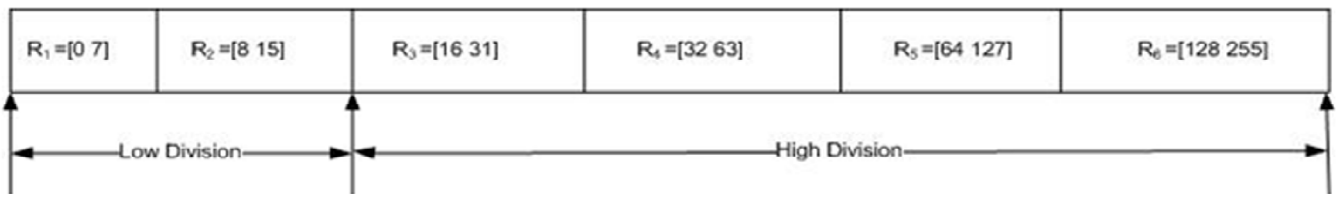


Figure 1: Division of range into low and high

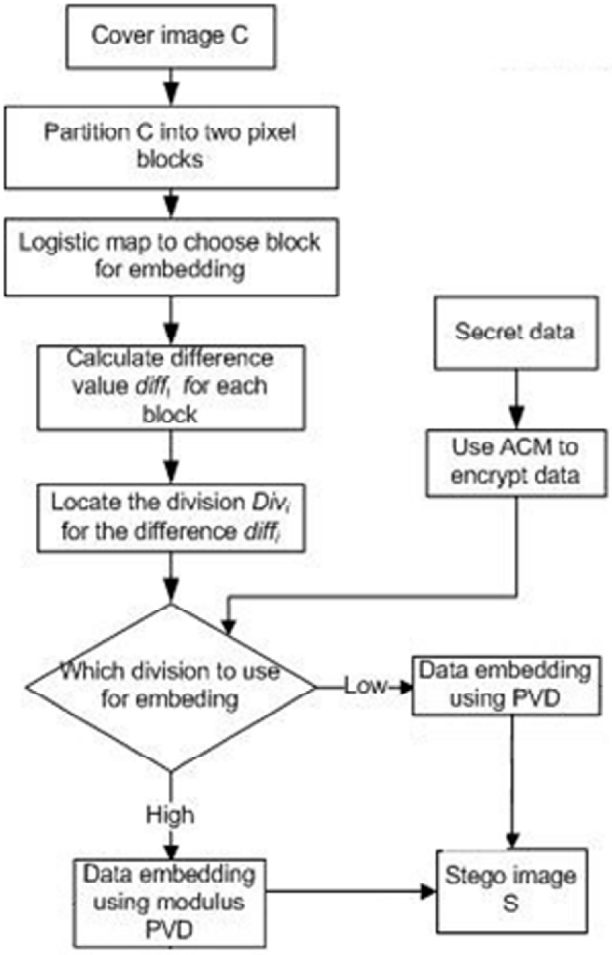


Figure 2: Block diagram of embedding algorithm

Step2: Use logistic map to generate pseudorandom sequence for choosing blocks for embedding

Step 3: Calculate the optimal range Ri of the diffi

$$Ri = \min(u_i - k)$$

Where u_ie"k

$$k = | diffi |$$

Step 4: if Ri belongs to low division, appropriate number of bits from secret data stream are read and transformed into binary value b;

For example, we consider a pixel block $[p_{(i,x)}\ p_{(i,y)}] = [100\ 200]$. So it lies in $R_5 = [64, 127]$ and let secret data is $(001100)_2$. Here $|diffi| = 100$, $w_i = 64$, b=10, diffi' = 42, m = 58, ceil m = 29, floor m = 29. As $P_i < P_{i+1}$ and diffi' < diffi so using case 4 of eqn. 4, $p_{(i,x)}$ '=100 + 29 = 129 and $p_{(i,y)}$' = 200-29 = 171. Finally replace [100 200] with [129 171] so as to embed 6 bit data $(001100)_2$ into the cover image.

Step 5: If Ri belongs to high-level, appropriate number of bits from secret data stream are read and transformed into binary value b.

For example, we consider a pixel block $[p_{(i,x)}\ p_{(i,y)}] = [255\ 110]$. So it lies in $R_6 = [128,255]$ and secret data is $(0011000)_2$. Here diff = 119, diff1 = 9 , $w_i = 128$, $P\_rem_i = 9$, $t'_i = 2^7 = 128$, m = 3,ceil m = 2, floor m = 1. As $P\_rem_i < t'_i$, diff>2^{ti}/2and $p_{(i,x)} > p_{(i,y)}$ and so by using case 7 of eqn. 7, $p_{(i,x)}$ '= 255-5=250 and $p_{(i,y)}$' = 110-4 = 106. Finally replace [255 110] with [250 106] so as to embed 7 bit data $(0011000)_2$ into the cover image.

2.2. The Extraction algorithm

For the extraction process the same range table is required as used in embedding process. The steps are simply reversed for obtaining secret data.

Step 1: the Stego-image is partitioned into blocks of two consecutive pixels, and the partition process is the same as embedding process.

Step 2: using Logistic map choose the blocks in the same order.

Step 3: the difference value diffi for each block of two consecutive pixels P_i' and P_{i+1}' is obtained.

Step 4: the optimal Ri for the diffi according to the original range table is obtained.

Step 5: if Ri belongs to the low-level the data is extracted using inverse PVD.

Step 6: if Ri belongs to the high level, the data is extracted using inverse modulus PVD.

Step 7: Using Cat's map reassemble the secret bit stream to generate the secret image.

3. EXPERIMENT AND RESULT

The proposed algorithm has been implemented on Matlab version 7.10.0.499 (R2013a). The quality measures against which the method is tested are PSNR, SSIM, Histogram attack, RS steganalysis and chi square attack. We have used standard test images of size 512 × 512 units for obtaining our results. We have set range table with widths w_i = {8, 8, 16, 32, 64, 128}. The test images are in lossless formats like bmp and tiff. The proposed approach has been compared with Wu et al's PVD method. For measuring imperceptibility we use PSNR and SSIM index. PSNR [13] is a very popular gauge for quantifying imperceptibility. It is measured in dB. Higher value of PSNR is aimed to be achieved as it indicates that more data can be fed into the cover without visual degradation of image. It is measured as

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

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)-y(i,j)\right)^2 \tag{11}$$

Here x(i,j) is the pixel of cover image and y(i, j) is the corresponding pixel of stego image.

Another measure for imperceptible target images that have been becoming popular is Structural Similarity index Map (SSIM)[14]. It takes into account the three measures of the human visual system (HVS) viz. luminance, contrast and structure and assumes the values in the range of 0 and 1. The values of constants C1 and C2 provide stability to the measure .x and y are same sized small image window.

$$SSIM = \frac{\left(2\times\overline{x}\times\overline{y}+C1\right)\times\left(2\times\sigma_{xy}+C2\right)}{\left(\sigma_x^2+\sigma_y^2+C2\right)\times\left(\left(\overline{x}\right)^2+\left(\overline{y}\right)^2+C1\right)} \tag{12}$$

3.1. Histogram analysis

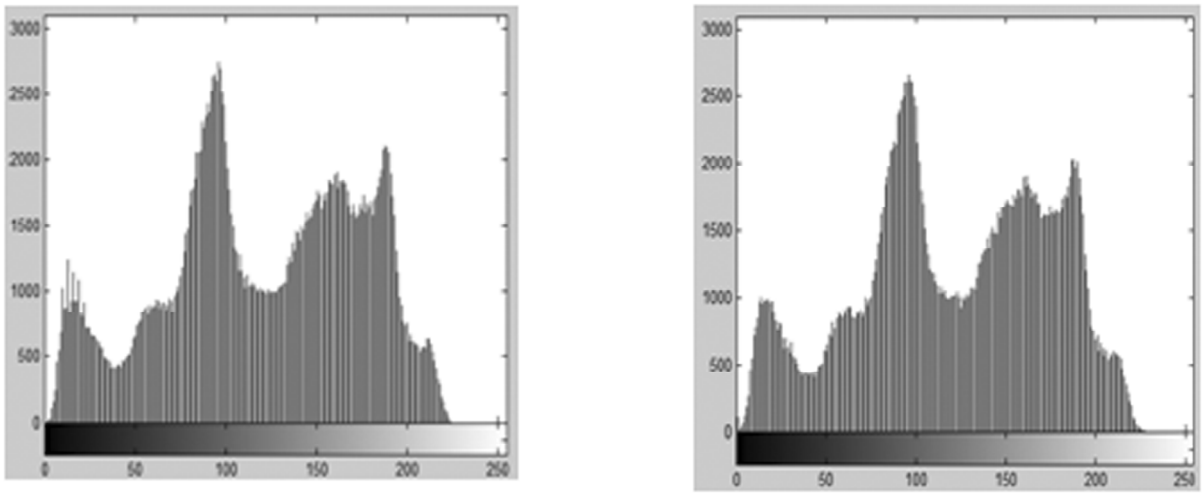
For the sake of visual inspection we plot histograms for both the cover and stego images. As the human eyes are unsusceptible to the changes after embedding, histogram is a useful tool for detecting any changes. If steps are visible in the generated plot of the histogram then it can be concluded that some hidden data is present in the stego image. Fig. 4 shows that the two histograms are very similar thus not raising any suspicion during visual inspection.

(a) **(b)**

Figure 3: Cover image and stego image
(a) Cover image peppers (b) Stego image after embedding secret data PSNR is 40.87 dB

Table 1
Comparison of results of the proposed and Wu Tsai's method.

Cover image512×512	*Wu Tsai's method*		*Our method*	
	PSNR(db)	*SSIM*	*PSNR(db)*	*SSIM*
Lena	37.98	0.9739	38.03	0.9765
Baboon	37.93	0.9864	39.42	0.9898
Peppers	38.74	0.9781	40.87	0.9943
Couple	36.77	0.9558	37.74	0.9837
Barbara	37.78	0.9858	39.60	0.9872
Elaine	34.84	0.9479	37.86	0.9892
Boat	39.88	0.9861	42.60	0.9942
plane	36.77	0.9599	39.89	0.9888
Tank	36.97	0.9597	39.75	0.9878
Bridge	35.88	0.9554	40.67	0.9911
Crowd	35.52	0.9557	36.57	0.9867



(a) Cover image **(b) Stego image**

Figure 4: Histograms for peppers

3.1.1. Security verification using statistical measures RS steganalysis and Chi square analysis

Following the embedding of secret data into the cover the next challenge that follows is to make the stego images indistinguishably alike to the cover image. The main aim of steganalysis techniques is to check and discover the existence of covert data into innocent host images. For this we have performed RS Analysis [15] and the values obtained are tabulated in Table 2. The analysis results that difference between RM (Positive Regular) and R-M (Negative Regular) is less than 10%. Furthermore, the difference between SM (Positive Singular) and S-M (Negative Singular) also is less than 10% thus concluding that the image is secured.

The Chi square attack analyzes the pair of values in the image. It tests whether the statistical properties of the image are altered or not as the embedding affects the histogram frequencies. Fig 5 shows that the probability of embedding is quite low for the cover peppers.

4. CONCLUSION

In this paper a hybrid steganographic method in spatial domain is proposed to embed secret into innocuous still images by using pixel value differencing and chaotic encryption techniques. This method treats the different regions of the image differently for hiding dat. The edges of images have more hiding capacity thus we use modulus PVD for such regions and the smooth regions are embedded using simple PVD. The experimental analysis of stego images exhibit that the proposed image has enhanced image quality as stated by higher PSNR and SSIM values and also is robust against statistical attacks as verified by RS steganalysis and Chi Square attack. Moreover visual imperceptibility is given away by histogram analysis.

Table 2
RS steganalysis of peppers

Positive Regular	0.3615
Positive Singular	0.4015
Negative Regular	0.4141
Negative Singular	0.2885

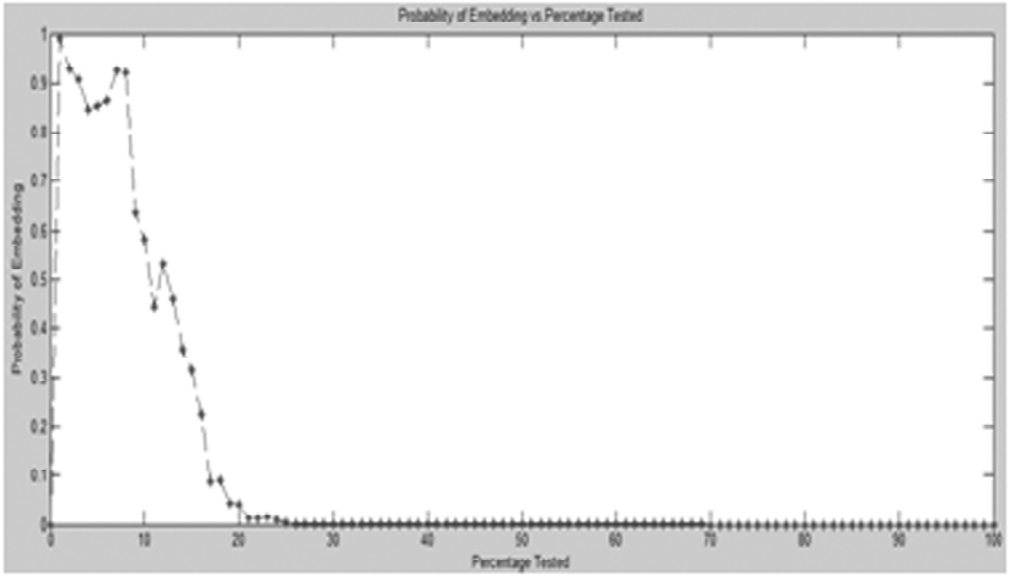


Figure 5: Chi square test for peppers

REFERENCES

[1] Book, I.J. Cox , M.L. Miller, J.A. Bloom, J. Fridrich & T. Kalker , "Digital Watermarking and Steganography", 2008.

[2] D.C. Wu & W.H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24,no. 9, pp.1613–1626, 2003.

[3] C.H. Yang, C.Y Weng , S.J Wang & H. M. 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, pp.488-497,2008.

[4] M. Gadiparthi ,K.Sagar, D. Sahukar & R. Chowdary , "A High Capacity Steganographic Technique based on LSB and PVD Modulus Method", International Journal of Computer Applications, Vol.22, no.5,pp. 8-11, 2011.

[5] X.Liao, Q.Y. Wen, & J.Zhang , "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", Journal of Visual Communication and Image Representation, Vol.22,no. 1, pp.1–8,2011.

[6] G. Swain , "Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution", Indian Journal of Science and Technology.Vol.7,no. 9, pp.1448–1454, 2014.

[7] M.S. Hwang, E.J.L. Lu & I.C. Lin, "A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem", IEEE Trans. Knowl. Data Eng., Vol.15, no.6, pp.1552–1560, 2003.

[8] Book, B. Schneier , "Applied cryptography", 1996.

[9] E.S. M. El-Alfy & A. A. Al-Sadi, "Improved Pixel Value Differencing Steganography Using Logistic Chaotic Map", International Conference on Innovations in Information Technology (IIT), pp. 129-133,2012.

[10] R. L.Tataru ,D. Battikh, S .El Assad, 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,pp.85-88, 2012.

[11] C.M. Wang , N.I .Wu, C.S. Tsai & M.S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", Journal of Systems and Software, Vol. 81,no.1,pp.150-158, 2008.

[12] G. Peterson, "Arnold's Cat Map", 1997.

[13] S. Zaghbani & R. Rhouma , "Data Hiding in Spatial Domain Image Using Chaotic Ma",5th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO), pp.1-5,2013.

[14] Z.Wang & A. C. Bovik , "Mean squared error: Love it or leave it? A new look at Signal Fidelity Measure", Signal Processing Magazine IEEE, Vol. 26, no. 1, pp. 98-117,2009.

[15] J. Fridrich, M. Goljan & R. Du, "Reliable Detection of LSB Steganography in Grayscale and Color Images", Proc. ACM, Special Session on Multimedia Security and Watermarking, pp.27–30, 2001.