Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 30 (2012) 36 – 44

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference on Communication Technology and System Design 2011

Horse Riding & Hiding in Image for Data Guarding

Thanikaiselvan V[a], Arulmozhivarman P[b], Rengarajan Amirtharajan[c], John Bosco Balaguru Rayappan[c], a*

[a,b]*School of Electronics Engineering, VIT University, Vellore, Tamilnadu, India*
[b]*School of Electrical & Electronics Engineering, SASTRA University, Tamilnadu, India*

Abstract

With the growing internet technology, science and requirement of concealing defense research work, there is a need for highly secured information exchange, which is the essence of steganography. Classic secret information could be undermined or even faked thereby, creating a menace to the core of secrecy. Steganography camouflages the hidden information into an unsuspicious digital file i.e. image, video or audio, thereby covering the existence of it. Using modified LSB substitution and readjustment procedure the mean square error has been reduced. Pixel indicator is used for increasing the embedding capacity of secret data. The security of secret data embedded into a cover file can be increased using random walk inside the file. In this paper we have used knight's tour for random walk, by not affecting the image quality. For high security while embedding, we randomize the three planes of RGB cover image using row vector, divide the image into four pixel blocks and then use Pixel value differencing (PVD) to embed data adaptively followed by knight's tour to select next block for embedding. This method gives highly secured and high capacity steganography

Keywords: Steganography; Row vector scrambling; Pixel indicator method; Modified LSB substitution

1. Introduction

In now-a-days more and more data (mainly digital) is transmitted into the web due to development in all major technical fields. Data in the form of images is livelier and visual communication is an effective method of sharing information. There is an increasing need for security of images which contain an embedded research work, designed weapons, information regarding any data which should not be revealed. Steganography is the area of science [1] which does this work (secret communication). The main goal of steganography is to hide secret information in cover file, so that no one can predict the

* Thanikaiselvan V. Tel.: +91-416-2202437; fax: +91-416-2243092.
E-mail address: thanikiselvan@vit.ac.in

1877-7058 © 2011 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2012.01.831

presence of secret information; the cover file and the secret data file can be any multi-media file i.e. image or video or audio file. Steganography, a branch of information security, several research works is being pursued to ensure high security.

Steganography hides the secret message and makes it invisible, while Cryptography [2] scrambles the message to make it unreadable, drawing the attention of eavesdroppers. A stego image is obtained after embedding secret data in cover medium, which modifies the cover image slightly. Stego objectives namely, imperceptibility, robustness and capacity of the hidden data, separate it from its relative techniques such as watermarking and cryptography [3]. Steganography is for preserving the privacy in secret communication, watermarking is for ownership protection and Cryptographic encryption is for data security.

Information hiding can be bifurcated into copyright marking and steganography [1, 3] which have gained impetus popularity in the recent past [3]. Furthermore these steganographic methods could be categorized into two types. The first type employs the spatial domain of a host image [1, 3-21] to camouflage secret data i.e. the secret data are directly embedded into the pixels of the host image [4-21]. Steganographic methods of the second type employ the transformed domain of a host image to hide secret data [22, 23]. Transformation functions like the discrete cosine transform (DCT) [22] or discrete wavelet transform (DWT) [23] are first maneuver to revamp the pixel values in the spatial domain to coefficients and then the secret data is embedded in the coefficients

The most common and well known method in steganography is Least Significant Bit-LSB substitution where the least significant n-bits of target pixel in cover image are embedded with message bits [4-21]. To improve this, many new optimized LSB approaches have been suggested [4, 5, 17, 20]. In some of these methods the concept of human vision is used to increase the quality of the stego images [4, 5, 17, 20], by embedding more bits in edge area than smooth area because human eye is more sensitive to smooth areas than edge areas[9-16, 18]. Chan and Cheng [4] proposed a simple LSB substitution along with optimal pixel adjustment process (OPAP). Wang [16] proposed a new adaptive least significant bit (LSB) substitution method using pixel-value differencing (PVD) that provides a high embedding capacity and imperceptible stego images. Wu and Tsai [10,12] proposed method to determine how many secret bits to be embedded based on difference value between two neighboring pixels. The capacity of secret bits to be embedded in target pixel using side match approach is proposed by Chang and Tseng [11].

Liao and Wen proposed a method using four pixel blocks differencing with a new LSB substitution method [9]. A combination of pixel-value differencing followed by LSB substitution is proposed by Wu et al [12]. Considering the minimum of two difference values in PVD method using adjacent pixels, a new method is proposed by Park et al. [13]. To determine how many secret message bits to be embedded a multi-pixel differencing method proposed by Yang and Weng uses four-pixel block PVD [14]. Using the modulus of two adjacent pixels to embed secret data, a method is proposed by Wang et al [16].

A comparative analysis of various image steganographic method is available in Amirtharajan *et al* [19]. Pixel Indicator based stego system proposed by Adnan Gutub[21] and its variant by Padmaa *et al* [20] Based on Randomization principle using LSB, where the secret is hidden in the least significant bits of the pixels, with more randomization in selection of the number of bits used and the color channels that are used. Another method of randomness through CDMA and OFDM using spread spectrum steganography available in [24, 25]. Kelley Seibel, explained how knight tour's[26-30] can be formed on the Cylinder and Torus in [26]. Knights tours blend with PVD based random image steganography is available in [30].Carefully analyzing all the aforementioned papers, the purposed technique provides random stego with high security and high PSNR. Randomizing the planes of colour image using row vector and using knight's tour to embed secret data randomly highly increases the security in this paper. This paper brings to limelight, the idea of hiding data within images and organized as follows. In Section 2 LSB embedding procedure is described. In Section 3 describes the proposed method. In Section 4, the experimental results are presented and discussed. Finally, the conclusions are presented in Section 5.

2. Review on literature

2.1 Randomization of Color Plane of Image

Let the total number of pixels be x in the RGB color image. Create a row vector of size x. Divide the row vector into k blocks. Each block, b_i contains p sub blocks (p = x/k). Here p is integer.

$$b_i = i + (k \times p') \qquad (1)$$

$$\text{Row vector} = [b_1\ b_2\ b_3\ b_4 \ldots\ldots\ldots\ b_k]$$

(2)

Where b_i represents i^{th} block of row vector ($1 \le i \le k$), p' represents position of sub block in each block ($0 \le p' \le (p-1)$).

Row vector gives the position of pixel to be considered for interchanging R, G, B pixel values. By considering different values for k, we can choose pixels in raster scan, column wise, and also randomly in the cover image. After performing the steps given below, the image will look like cover image with changes in color of image. By using this randomization of color plane of image we can achieve high security.

Divide each element of the row vector by 3, and do the following operation on color plane of corresponding pixel of cover image:

- If reminder is 0, leave the pixels as it is.
- If reminder is 1, interchange the R & G color plane pixel value.
- If reminder is 2, replace R by B, G by R and B by G plane pixel value.

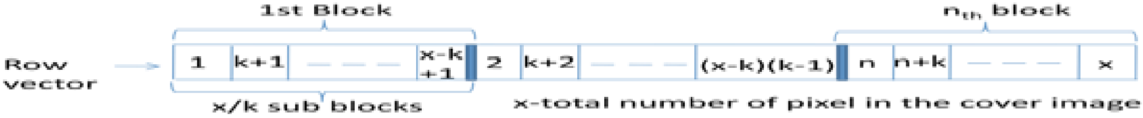
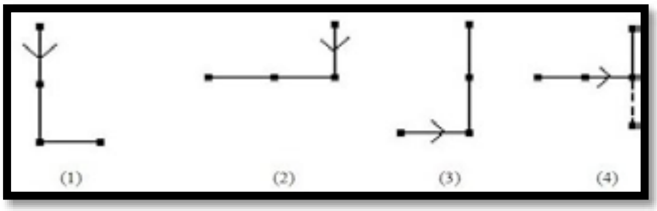


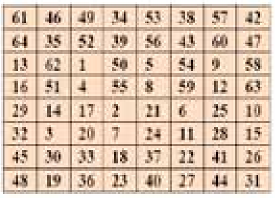
Fig 1: The row vector to be considered for randomization of color plane of image.

Fig. 2. (a) Image before the randomization of colour plane (b) Image after the randomization of colour plane

2.2 Knight's Tour:

In a n × n chessboard if the knight travels all squares only once is called Knight's tour shown in Figure 3. In open knight's tour the last square is not a valid knight's move to the first square, but in closed (cyclic) knight's tour it is a valid knight's move. Travelling two squares vertically and one square horizontally or two squares horizontally and one square vertically i.e. making an 'L' shape move is a valid knight move. Euler first made the mathematical analysis of the problem in 1759. Then research has started in finding the number of possible knight's tours for a given n × n matrix. Not every square matrix is having knight's tour till now. Kelley Seibel [24] in his research work suggested that, by assuming the square matrix as cylinders and torus, we can get more possible knight tours. 13,267,364,410,532 are the number of cyclic knight's tour in an 8 × 8 matrix calculated by Lobbing and Wegener [29]. But the actual number can be greater. In this paper the concept of knight's tour considering the square matrix as a cylinder is used to embed the secret data along the knight's move. Using this idea high security can be achieved in steganography since the search space will be significantly high even if we know the starting square of knight's move for 8 × 8 is shown in Fig. 4.





61	46	49	34	53	38	57	42
64	35	52	39	56	43	60	47
13	62	1	50	5	54	9	58
16	51	4	55	8	59	12	63
29	14	17	2	21	6	25	10
32	3	20	7	24	11	28	15
45	30	33	18	37	22	41	26
48	19	36	23	40	27	44	31

Fig. 3. Cyclic order for closed knight's tour for n1 × n2 matrix.

Figure 4: knight's tour on 8 × 8 cylinder

3. Proposed methodology

Randomization of colour planes is done in cover image using row vector for high security. Edge area pixels can endure more number of secret bits than in smooth areas without any perceptual distortion. Pixels in cover image blocks are embedded with secret data bits by n-bit modified least significant bits (MLSB) substitution, n is decided by average difference value of the block whether it belongs to smooth (nl) or edge area (nh). To reduce perceptual distortion we go for readjustment procedure, by which we make sure that average difference value will be in same level even after embedding the secret data to cover image. To improve security the secret data is embedded randomly in cover image using knight's tour. Embedding process and extraction process are as follows:

Embedding algorithm

A colour image is taken as cover image. The cover image is divided into blocks of four pixels which do not overlap with each other. For each block there will be four pixels $x_{i,j}$, $x_{i,j+1}$, $x_{i+1,j}$, $x_{i+1,j+1}$ and their gray values g_o, g_1, g_2 and g_3 respectively. The detailed steps in embedding procedure are given below:

STEP-1: Create a row vector of size equal to number of pixels in one color plane of cover image (Let x). Divide this into k blocks. Each block, b_i contains p sub blocks (p = x/k), here p is integer.

$$b_i = i + (k \times p')$$

$$\text{Row vector} = [b_1\ b_2\ b_3\ b_4 \ldots\ldots\ldots\ b_k]$$

Where b_i represents i^{th} block of row vector ($1 \leq i \leq k$), p' represents position of sub block in each block ($0 \leq p' \leq (p-1)$).

STEP-2: Divide each element of row vector by 3.

- If reminder is 0 no change in colour plane.
- If reminder is 1, interchange R & G colour plane pixel value.
- If reminder is 2, do the following- Replace R plane by B plane, G plane by R plane, B plane by G plane pixel value.

Repeat this for all pixels of cover image.

STEP-3: Divide each colour plane of image into non overlapping blocks of four pixels.

STEP-4: Decide the four pixel block to be chosen for embedding by using knight's path by giving the position of starting point of knight's tour.

STEP-5: Divide Blue plane component of the first pixel of the block chosen in previous step by 4.

- if reminder is 0, perform the operation given in step 5-10 first on R-plane then on G-plane.
- If reminder is 1, perform operation given in step 5-10 on G-plane.
- If reminder is 2, perform operation given in step 5-10 on R-plane.
- if reminder is 3, perform the operation given in step 5-10 first on G-plane then on R-plane.

STEP-6: Calculate the average difference value Δ, which is given by

$$\Delta = \frac{1}{3}\sum_{i=0}^{3}(g_i - g_{\min}) \quad (3)$$

where $g_{\min}=\min\{g_0,g_1,g_2,g_3\}$; g_0,g_1,g_2,g_3 are the pixel values.

STEP-7: Our proposed method adaptively embeds message using two levels (lower level and higher-level).If $\Delta \leq th$, Δ belongs to ''lower-level" (i.e., the block belongs to smooth area) then $n = n_l$. Otherwise, Δ belongs to ''higher-level" (i.e., the block belongs to an edge area), then $n = n_h$, satisfying $2^{n_l} \leq th \leq 2^{n_h}$ and $1 \leq n_l , n_h \leq 5$

STEP-8: Verify whether the block belongs to ''Error Block". If not, continue to next step. Otherwise, restart from Step 4.

ERROR BLOCK:

Assume $g_{\max} = \max \{g_0, g1, g2, g3\}$ the block is called ''Error Block" if and only if $D \leq th$ and $g_{\max} - g_{\min} > 2\times th + 2$ e.g., Let th = 5,and block be (216, 217, 216, 230) belongs to ''Error Block", because and 230 - 216 = 14 > 2×5+2 = 12 .

STEP-9: Convert g_i to g_i' by embedding n message bits in LSB part of all four pixel.

STEP-10: Apply the n-bit modified LSB substitution method to g_i', and let g_i'' be the result ($0 \leq i \leq 3$), respectively.

STEP-11: This step is called ''readjusting procedure". Let $\hat{g}_i = g_i'' + \ell \times 2^n$, ($0 \leq i \leq 3$), $\ell \in \{0,1,-1\}$, and search for ($\hat{g}_0$, $\hat{g}_1$, $\hat{g}_2$, $\hat{g}_3$) such that

$$\hat{\Delta} = \frac{1}{3}\sum_{i=0}^{3}(\hat{g}_i - \hat{g}_{\min}) \quad (4)$$

- $\hat{\Delta}$and Δ belong to same level,
  - where $\hat{g}_{\min} = \min\{\hat{g}_0 , \hat{g}_1 , \hat{g}_2 , \hat{g}_3\}$
- The final stego block ($\hat{g}_0$, $\hat{g}_1$, $\hat{g}_2$, $\hat{g}_3$) does not belong to ''Error Block".
- The value of $\sum_{k=0}^{3}(\hat{y}_i - y_i)^2$ [MSE] is minimized.

After the replacement of (g_0, g_1, g_2, g_3) by ($\hat{g}_0$, $\hat{g}_1$, $\hat{g}_2$, $\hat{g}_3$) in the block, the purpose of 4k-bit secret data hiding have been achieved. Repeat Steps 4–10 until all the blocks of cover image are covered.

STEP-12: Repeat step-1 once again to get final stego image.

Extraction algorithm

The secret bits can be extracted directly from the stego image. For extraction divide the stego image into non-overlapping four pixel block as done in embedding process. Let the four neighbouring pixels be g_o, g_1, g_2 and g_3. Use following steps to extract the secret data:

STEP-1: Perform operations given in step-1 to 4 in embedding algorithm.

STEP-2: Divide Blue plane component of the first pixel of the block by 4, if reminder is 0, perform the operation given in step 3-6 first on R-plane then on G-plane., if reminder is 1, perform operation given in step 3-6 on G-plane, if reminder is 2, perform operation given in step 3-6 on R-plane, if reminder is 3, perform the operation given in step 3-6 first on G-plane then on R-plane.

STEP-3: Find average difference value Δ.

STEP-4: Find the level in which Δ lies by using the threshold (th). If Δ lies in lower level $n = n_l$, if it lies to higher level $n=n_h$.

STEP-5: Check the block for error. If it is an error block go to the step 2, else go to next step i.e. step 6.

STEP-6: Extract the 4n secret bits from n bit LSB of pixels ($0 \leq i \leq 3$).

STEP-7: Choose next block from which data has to be extracted using Knight's Tour and then again perform step 2-6 on the 2 × 2 block to extract embedded data.

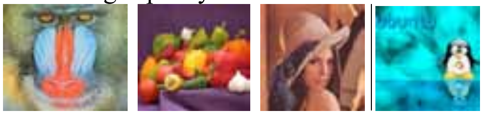
STEP-8: Repeat this process till all the blocks covered to retrieve entire secret data.

4. Results & Discussion

To evaluate the performance of our proposed method several experiments are performed. Four colour images are taken with size 256 × 256 as cover images which are shown in Fig. [1-4]. Our proposed method considers 2 × 2 blocks which do not overlap each other, and the edge features are considered that is the edge area pixels can endure more changes having less visual distortion. A large text is taken as secret data, which is converted in digital format that is in ones and zeroes and they are embedded into cover image. To evaluate the quality of the stego image peak signal to noise ratio (PSNR) is used, which is defined as given below, for an M × N grayscale image.

$$PSNR = 10 * \log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{i=1}^{N} \left(p_{i,j} - q_{i,j}\right)^2}$$

Where $p_{i,j}$ and $q_{i,j}$ denote the cover image pixels and stego image pixels, respectively. Using the proposed method the stego images with different values of th, n_l and n_h after adding secret data are shown in Figs. 2-4. Changes due to data embedding in these figures are imperceptible to human vision. Several experiments have been carried with different values of n_l, n_h and threshold. For example, consider th = 12, 2–4 division with Δ, if the block is having average difference value (Δ) less than threshold level then 2-secret message bits are embedded in each pixel of that block and if it is greater than threshold level then 4-secret message bits are embedded in each pixel of that block using modified LSB substitution method. The results of proposed method are shown in Table 1-2 with embedding capacity and PSNR values for different n_l, n_h, and threshold values for different cover images. The capacity of embedded data is almost four times the capacity shown in Table 1-2 with almost same PSNR, if we use image of size 512×512 instead of 256×256 cover image. We randomized the colour channels of each pixel using row vector and used knight's tour for embedding secret data randomly in cover image. This allows us to achieve high security, also high embedding capacity has been achieved.

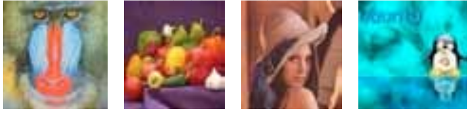


(a) (b) (c) (d)

Fig 1. Four cover images of size 256 × 256; (a) baboon, (b) peppers, (c) Lena.(d) Ubuntu

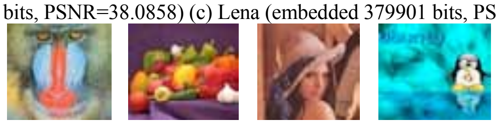
(a) (b) (c) (d)

Fig 2. Four stego images (th=7 nl=2,nh=3) (a) baboon (embedded 292233 bits, PSNR=43.7689db) (b) peppers (embedded 294657 bits, PSNR=43.8640) (c) Lena (embedded 291865 bits, PSNR= 43.8011) .(d) Ubuntu (embedded 290895 bits, PSNR=44.9469)



(a) (b) (c) (d)

Fig 3. Four stego images (th=15, nl=3, nh=4) (a) baboon (embedded 381701 bits, PSNR=37.9942db) (b) peppers (embedded 389789 bits, PSNR=38.0858) (c) Lena (embedded 379901 bits, PSNR= 38.1208) (d) Ubuntu (embedded 389213 bits, PSNR=39.0791)



(a) (b) (c)

Fig 4. Four stego images (th=21, nl=4, nh=5) (a) baboon (embedded 449153 bits, PSNR=32.5056db) (b) peppers (embedded 480633 bits, PSNR=32.0985) (c) Lena (embedded 469425 bits, PSNR= 32.4334) (d) Ubuntu (embedded 486581 bits, PSNR=33.1195)

Table 1 Result of proposed algorithm with two different Th and k_l-k_h (i.e. 7, 2-3 & 12, 2-4)

Cover (256×256)	T=7,2-3					T=12,2-4				
	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR
Lena	291865	42.05	43.75	46.83	43.8011	377033	36.25	38.10	41.33	38.0938
Baboon	292233	42.03	43.75	46.72	43.7689	380361	36.22	37.95	40.96	37.9686
Peppers	294657	42.11	43.81	46.93	43.8640	385897	36.42	37.97	40.98	38.0818
Ubuntu	290895	44.56	43.92	46.87	44.9469	383785	38.63	38.09	41.09	39.0921

Table 2 Result of proposed algorithm with two different Th and k_l-k_h (i.e. 15, 3-4 & 18, 2-5)

Cover (256×256)	T=15,3-4					T=18,2-5				
	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR
Lena	379901	36.30	38.10	41.33	38.1208	442793	30.66	32.49	35.79	32.5056
Baboon	381701	36.28	37.98	40.89	37.9942	449153	30.63	32.23	35.14	32.2984
Peppers	389789	36.40	38.02	40.99	38.0858	469649	30.46	31.95	35.02	32.0985
Ubuntu	389213	38.60	38.07	41.11	39.0791	475745	32.72	32.24	35.24	33.2206

Table 3 Result of purposed algorithm with two different Th and kl-kh (i.e. 18, 3-4 & 21, 4-5)

Cover (256×256)	T=18,3-4					T=21,4-5				
	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR	capacity	RED PSNR	GREEN PSNR	BLUE PSNR	Overall PSNR
Lena	375845	36.42	38.29	41.49	38.2707	469425	30.61	32.42	35.65	32.4334
Baboon	377237	36.23	37.95	40.880	37.9647	469577	30.63	32.16	35.12	32.2718
Peppers	387737	36.41	37.99	41.01	38.0862	480633	30.43	31.95	35.00	32.0790
Ubuntu	388845	38.52	38.07	41.07	39.0391	486581	32.59	32.14	35.18	33.1195

5. Conclusion

In this paper we have proposed a steganographic method based on four-pixel block differencing, modified LSB substitution and knight's tour. Using modified LSB substitution and readjustment procedure the mean square error has been reduced. The security of secret data embedded into a cover file can be increased by random walk inside the file using knight's tour for random walk, by not affecting the image quality. For high security we use pixel indicator method of embedding and randomized the three planes of RGB cover image using row vector. Results show that our proposed method has provided a greater security with high embedding capacity and a better image quality. In steganography, the embedding capacity, robustness to attacks like steganalysis and imperceptivity form a magical triangle. That is if we want high embedding capacity (like 486581 bits) and good image quality (33.11dB) it would sacrifice on the robustness a little bit.

REFERENCES

[1] Katzenbeisser S, Petitcolas FAP. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[2] Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods , *Information Sciences, 2010;* **90 :** 727– 752.

[4] Chan CK, Chen LM. Hiding data in images by simple LSB substitution, *Pattern Recognition,* 2004;**37** : 469–474.

[5] Thien CC, Lin JC. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, *Pattern Recognition*, 2003; **36**: 2875–2881

[6] Bender W, Gruhl D, Morimoto N, Lu A. "Techniques for data hiding" *IBM Syst. J.* 1996; **35** 313–336.

[7] Lin C, Lin YB, Wang CM. Hiding data in spatial domain images with distortion tolerance, *Comput.Stand. Inter*. 2009; **31**: 458–464.

[8] Amirtharajan, R.; Balaguru, R.J.B, Tri-Layer Stego for Enhanced Security – A Keyless Random Approach - *in IEEE International Conference on Internet Multimedia Services Architecture and Applications* (IMSAA), 2009; p.1–6.

[9] Xin Liao, Qiao-yan Wen, Jie Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, *J. of Visu. Communic. and Image Representation*, 2011; **22**:1–8.

[10] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing, *Pattern Recognit. Lett*. 2003; **24**: 1613–1626.

[11] Chang CC, Tseng HW. A steganographic method for digital images using side match, *Pattern Recognit. Lett.* 2004; **25**: 1431–1437.

[12] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods, *Proc. Inst. Elect.Eng., Vis. Images Signal Process* 2005;**152** : 611–615.

[13] Park YR, Kang HH, Shin SU, Kwon KR. A Steganographic Scheme in Digital Images Using Information of Neighboring Pixels, LNCS: 3612, *Springer-Verlag,Berlin, Germany*, 2005. p. 962–967.

[14] Yang CH, Weng CY. A steganographic method for digital images by multipixel differencing, *in: Proceedings of International Computer Symposium,Taipei, Taiwan, R.O.C.*, 2006; p. 831–836.

[15] Jung, K.J. Ha, K.Y. Yoo, Image data hiding method based on multi-pixel differencing and LSB substitution methods, in: International Conference on Convergence and Hybrid Information Technology, 2008; p. 355–358.

[16] Wang CM, Wu NI, Tsai CS, HwangMS. A high quality steganography method with pixel-value differencing and modulus function, *J. Syst. Softw.* 2008;**81**: 150–158.

[17] Wang RZ, Lin CF, Lin JC, Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition* 2000; **34** : 671– 683

[18] Yang CH, Weng CY, Wang SJ, Sun HM, Adaptive data hiding in edge areas of images with spatial LSB domain systems, *IEEE Trans. Inf. Forensics Secur.* 2008;**3**: 488–497.

[19] Amirtharajan R, Akila R, Deepikachowdavarapu P. A Comparative Analysis of Image Steganography*, International journal of computer applications, 2010;* **2**: 41– 47.

[20] Padmaa M, Venkataramani Y, Rengarajan Amirtharajan, Stego on 2^n:1 Platform for Users and Embedding. *Information Technology Journal*, 2011;**10**: 1896–1907.

[21] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, Pixel Indicator high capacity Technique for RGB image Based Steganography, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[22] Provos N, Honeyman P. Hide and seek: An introduction to steganography, *IEEE Security Privacy Mag*, 2003;1: 32–44.

[23] Thanikaiselvan V, Arulmozhivarman P, Amirtharajan, Rengarajan , John Bosco Balaguru Rayappan, "Wave(Let) Decide Choosy Pixel Embedding for Stego" IEEE Conference on Computer, Communication and Electrical Technology ICCCET 2011, (2011) 157 - 162 D.O.I 10.1109/ICCCET.2011.5762459

[24] Amirtharajan R., Rayappan, John Bosco Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. IEEE Wireless ViTAE Conference India. (2011) DOI: 10.1109/WIRELESSVITAE.2011.5940912

[25] Kumar P P, Amirtharajan R, Thenmozhi K, Rayappan JBB. Steg-OFDM blend for highly secure multi-user communication, IEEE Wireless ViTAE Conference India (2011) DOI:10.1109/WIRELESSVITAE.2011.5940918

[26] Kelley Seibel, The Knight's Tour on the Cylinder and Torus, Research experience for Undergraduates, Dept. of Mathematics, Oregon State University, August, 1994.

[27] Mordecki. E., "On the Number of Knight's Tours, "Prepublicacion es de Malem6tica de la Universidad de la Repliblica, 2001l57. 2001.

[28] Gordon VS, Slocum TJ, The Knight's Tour Evolutionary vs. Depth-First Search,IEEE Congress on Evolutionary Computation(CEC'04), Portland, Oregon (2004).

[29] Lobbing. M. and Wegener. I., "Branching Programs and Binary Decision Diagrams. Weory and Applications." In SIAM Monographs on Discrete Mathematics and Applications. Philadelphia, PA, 2000.

[30] Thanikaiselvan V, Santosh Kumar, Narala Neelima, Rengarajan Amirtharajan, “Data Battle on the Digital Field between Horse Cavalry and Interlopers”, *Journal of Theoretical and Applied Information Technology*, 2011; **29 :** 85 – 91.