Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DATA BATTLE ON THE DIGITAL FIELD BETWEEN HORSE CAVALRY AND INTERLOPERS

[1]THANIKAISELVAN V, [2]SANTOSH KUMAR, [2]NARALA NEELIMA, [3]RENGARAJAN AMIRTHARAJAN

[1]Asstt Prof(Sr)., Communication Engg. Division/SENSE, VIT University, Vellore, India-632014

[2]Final Year Students., Department of ECE/SENSE, VIT University, Vellore, India-632014

[3]Asstt. Prof (III)., Department of Electronics & Communication Engineering, School of Electrical & Electronics Engineering, SASTRA University, Thanjavur, India -613401

ABSTRACT

In this paper a novel steganographic method has been proposed to improve the security of embedded data with high capacity and imperceptible visual quality, the proposed method is based on four-pixel block differencing, modified LSB substitution and Knights tour. Secret data is embedded randomly using knights tour in each 8×8 pixels block of cover image and n-bit modified LSB substitution has been used to improve the quality of stego image, where n is decided by the level to which the average difference value falls into, then it employs readjustment procedure to reduce the perceptual distortion. The proposed method adaptively embeds the secret data into cover image by differentiating the edge and smooth areas, so that more number of secret bits can be embedded without making any perceptual distortion. Results show that our proposed method has provided greater security with high embedding capacity and a better image quality.

Keywords: *Information hiding, Steganography , Modified LSB substitution, Knights tour, Pixel Value Differencing (PVD)*

1. INTRODUCTION

The commodity most freely available in today's generation is "information". And it isn't a surprising fact since; mankind has thrived on information ever since they have evolved, from pre-historic times of carvings on walls of caves to the present age "within-seconds" data transfer between two different continents. With Science and Technology providing assistance for information flow too, on a large scale there has been a literal boom in the field of communication. But along with the pros comes the cons, while information exchange and growth are escalating, there has been an equal rise in espionage, infringement and eaves-dropping on it, especially when the data concerned is highly sensitive as in the case of military, banks or security systems. Thus, has behooved the need to device methods for protecting it, and thus has grown an entire dimension known as "information hiding" which provides clandestine means of transmitting information. It includes cryptography, steganography and digital water marking.

While cryptography [1] is the ancient art of writing messages, by scrambling them and presenting them in a manner unrecognizable by parties other than the recipients and senders, steganography involves hiding the data to be transmitted to be encapsulated in an outer cover which could be audio, video, pictures, etc. in such a manner that it is inconspicuous to the eavesdroppers. And that's where steganography[2, 3] gains the upper hand over cryptography, since cryptography gives a hint to the hackers that secret data is being transmitted, giving them a pin point to the vulnerability of the system. The dexterity with which data can be hidden in this technique is unparalleled and is the most efficacious one present.

In addition to the requirement of security, equally pressing demands are presented, for, the steganography system is being robust and having a high data capacity known as "payload" [2]. In general, a system is considered to be suitable for "information hiding "when it satisfies the three requirements of Friedrich's triangle, i.e. imperceptibility, robustness and high capacity. Furthermore, steganography can be classified into spatial domain [4-17] and transform domain steganography [18-21].

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the spatial domain [4-17], data is hidden in the system by direct manipulation of the pixels, the most common of them being normal LSB substitution method, while in the transform domain techniques, the image is first transformed using techniques like discrete cosine transform (DCT)[18,19] or discrete wavelet transform (DWT)[20,21], and then the coefficients are exploited for the purpose of data concealment.

2. RELATED WORKS

In the recent past, many steganographic methods have been proposed [2-21], Chan and Cheng proposed a simple LSB substitution along with optimal pixel adjustment process (OPAP) [4] , then Yang [12] came up with a modification of pixel-value differencing (PVD) along with LSB method to provide a high embedding capacity and imperceptible stego images. Wu and Tsai [6] used Pixel Value Differencing (PVD) for embedding data in pixels while the number of bits to be embedded in a pixel using side match approach is proposed by Chang and Tseng [7].

A combination of pixel-value differencing and LSB substitution is proposed by Wu *et al* [10]. Based on the difference value between two, three and four pixels adjacent to the target pixel a new method is proposed by Park et al. [11]. To determine the number of secret bits to be embedded a multi-pixel differencing method proposed by Yang and Weng uses three difference values by considering a four-pixel block [12].

A detailed survey on digital image steganography methods found in [3,8]. A steganographic method that uses the remainder of two consecutive pixels to embed secret data is proposed by Wang *et al* [10]. To differentiate between edge areas and smooth areas Yang *et al* [15] used the difference between two consecutive pixels but its drawback was less embedding capacity and low stego image quality.

A comparative analysis of various image steganographic methods is available in Amirtharajan *et al* [12]. Padmaa *et al* [14] proposed a method to embed secret data by adapting zig-zag traversing path using pixel value differencing. Liao and Wen proposed four pixel differencing and modified LSB substitution and achieved better stego image quality with high embedding capacity [14].

On review of all the past works, our new methodology proposed, reinforces the security of the stego-image, making it highly imperceptible by improving the four-pixel differencing method significantly and including the knight's tour as a method of traversing through the image for data hiding in gray scale images.

2.1 Knights Tour

In a n × n chessboard if the knight travels all squares only once is called Knight's tour [22-24]. 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 [22] 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 a 8 × 8 matrix calculated in [25]. 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.

Even though there are no circuits on the n1 × n2 (n1 and n2 are even numbers and n1 ≥ 4) cylinder, the following is an algorithm which gives a tour for the n1 × n2 cylinder. Start with any square in the matrix. Then move two squares down and one square to the right. Next, go one square down and two square to the left. Then, move one square to the right and two squares upward. Finally, move two square rights and one square up. If the upper square is already visited then move one square down instead of one up. Repeat this cyclic steps until all the squares are visited.

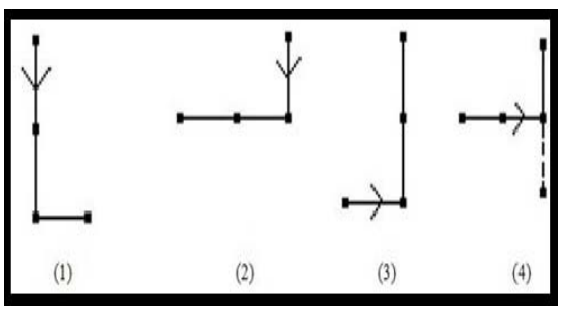


Figure 1: cyclic order to be followed for closed knight's tour for n1 × n2 matrix.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

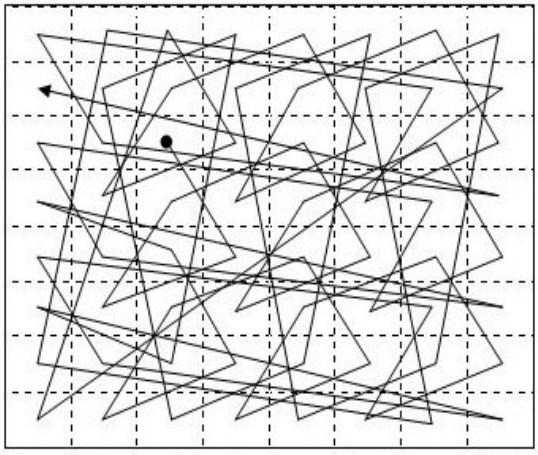


Figure 1.1 Completed knight's tour on the 8 × 8 cylinder.

3. PROPOSED METHODOLOGY

It is a known fact that visual perception is very accurate and can get easily affected by any minor changes or defects in a picture, and on this basis it is noted that more data can be embedded in the edge pixels rather than pixels in smooth areas, with very high levels of imperceptibility. Thus we adopt a Modified n-bit Least Significant Bits (MLSB) where n would be decided by the average difference value of the block whether it belong to smooth(n1) or edge area(n2). Readjustment of the picture is first done so as to maintain the average value difference more or less similar before and after embedding of data.

3.1 Embedding algorithm

Step 1: The 8-bit gray scale image, i.e. cover image is taken.

Step 2: The image is then divided into 4 pixel block , the four pixels to be taken for embedding are determined by employing knight's path by giving the position of starting of knight's tour, so as they do not overlap, let them be $x_{i,j}$, $x_{i,j+1}$, $x_{i+1,j}$, $x_{i+1,j+1}$ and their gray values g_0, g_1, g_2 and g_3 respectively.

Step 3: The average difference value Δ is calculated using the formula:

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

Here g_{min} = min (g_0, g_1, g_2, g_3)

Step 4: A threshold value (th) is determined. If $\Delta \leq$ th, n = nl (lower level) and if $\Delta >$ th, n = nh (higher level). The lower level belongs to the smooth pixels region and the higher level belongs to the edge pixels region.

Step 5: The readjustment procedure follows the range of nl, nh, and should be $2^{nl} \leq$ th $\leq 2^{nh}$ and $1 \leq$ nl, nh ≤ 5

Step 6: A block is said to be error block if $\Delta \leq$ th and $(g_{max} - g_{min}) \geq 2\times th+2$, Where g_{max}= max (g_0, g_1, g_2, g_3), verify whether the present block is not an error block, if not, proceed to the next step, else restart from the beginning. An error block is never used for embedding message bits.

Step 7: LSB substitution is used for embedding secret data, in each four pixel block.

Step 8: Then, MLSB is employed on the obtained result. Let the output of this stage is g_i" for $(0 \leq i \leq 3)$ respectively.

Step 9: In this step we readjust the pixels value obtained from previous step. Assume $\hat{g}_i = g_i" + l \times 2n$, $0 \leq i \leq 3$, $l \in (-1, 0, 1)$, find a combination of $\hat{g}_i$ $(0 \leq i \leq 3)$ according to the following conditions:

a. Δ and $\hat{\Delta}$ should lie in same level,

$$\hat{\Delta} = \frac{1}{3}\sum_{i=0}^{3}(\hat{g}_i - \hat{g}_{\min}) \qquad (2)$$

Where $\hat{g}$min=min ($\hat{g}$0, $\hat{g}$1, $\hat{g}$2, $\hat{g}$3).

b. The resultant block should not be an error block.

c. The MSE $\sum_{i=0}^{3}(\hat{g}_i - g_i)^2$ of the resultant block would be minimum.

Step 10: Now replace (g_0, g_1, g_2, g_3) by ($\hat{g}_0$, $\hat{g}_1$, $\hat{g}_2$, $\hat{g}_3$).

Step 11: On this entire process, 4n data bits would be clandestinely embedded into the block is 2×2 pixels.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 Extraction algorithm

Step 1: Get the 8-bit stego image.
Step 2: Repeats steps 1 to 3 as shown in the embedding algorithm.
Step 3: Determine average difference value Δ.
Step 4: On calculation determine if Δ lies in lower level n = nl, or if it lies in higher level n=nh.
Step 5: Check if its an error block, if not go ahead else restart.
Step 6: Extract the 4n secret bits from n bit LSB of pixels $g_i (0 \le i \le 3)$.
Step 7: Choose next block to be extracted by using Knight's tour and start from step-3.
Step 8: Repeat this process till you obtain the entire secret data.

4. RESULTS & DISCUSSION

To evaluate the performance of our proposed method several experiments are performed. Three gray scale images are taken with size 256 × 256 as cover images which are shown in Fig. [1-4]. Our proposed method considers 2 × 2 non overlapping pixel blocks instead of two consecutive pixels, so the edge features may be considered sufficiently and the pixels in edge areas can endure much more changes without having perceptible 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

(a) (b) (c)

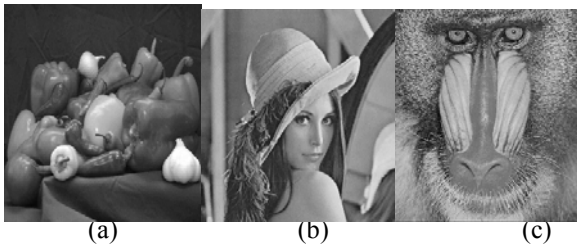
Fig 1. Three cover images of size 256 × 256; (a) peppers, (b) Lena, (c) baboon.

(a) (b) (c)

Fig 2. Three stego images (th=12 nl=2,nh=4) (a) peppers (embedded 149497 bits, PSNR= 41.5409db) (b) Lena (embedded bits 165009, PSNR=39.6740 db) (c) baboon (embedded 226089 bits, PSNR=35.9403 db)

(a) (b) (c)

Fig 3. Three stego images (th=15, nl=3, nh=4) (a) peppers (embedded 203293 bits, PSNR= 39.4533db) (b) Lena (embedded bits 209937, PSNR=38.5336 db) (c) baboon (embedded 238653 bits, PSNR=35.9483db)



(a) (b) (c)

Fig 4. Three stego images (th=18, nl=3, nh=4) (a) peppers (embedded 201868 bits, PSNR=39.6758db) (b) Lena (embedded bits 207145, PSNR=38.8837db) (c) baboon (embedded 234373 bits, PSNR=36.2527db)

used, which is defined as given below, for an M × N grayscale image.

$$PSNR = 10 * \log_{10}\left(\frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{i,j} - q_{i,j})^2}\right) \quad (3)$$

Where pi,j and qi,j denote the pixel values in row i and column j of the cover image and the stego image, respectively. The stego images obtained by our proposed method with various values of th, nl and nh are shown in Figs. 2-4. Changes due to data embedding in these figures are imperceptible to human vision i.e. the proposed method has overcome distortions resulted from embedding high capacity secret data. We experimented for different values of nl, nh and threshold values. For example, consider 2–4 division with k=16, th = 12, which means that four-pixel block having average difference value in low level ,will be embedded by 2-bits and in high level, will be embedded by 4-bit modified LSB substitution method. The results of proposed method are shown in Table 1-2 with embedding capacity and PSNR values for different nl, nh, 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.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1 Comparison of experimental result between Xin Liao and ours

Cover (256×256) k=16	th=7,2-3			th =12,2-4			th =15,3-4		
	capacity	Xin Liao PSNR	ours PSNR	capacity	Xin Liao PSNR	ours PSNR	capacity	Xin Liao PSNR	ours PSNR
Cameraman	152209	43.6001	43.5972	162657	39.9307	39.9647	209825	38.5596	38.5662
Lena	158905	42.8883	42.9083	165009	39.6749	39.6740	209937	38.5782	38.5336
Baboon	187761	41.0838	41.0551	226089	35.9645	35.9403	238653	35.9492	35.9483
Peppers	147505	44.0014	43.9822	149497	41.5408	41.5409	203293	39.4613	39.4533

Table 2 Comparison of experimental result between Xin Liao and ours

Cover (256×256) k=16	th =18,2-5			th =18,3-4			th =21,4-5		
	capacity	Xin Liao PSNR	ours PSNR	capacity	Xin Liao PSNR	ours PSNR	capacity	Xin Liao PSNR	ours PSNR
cameraman	164533	35.899	35.8292	207557	38.8447	38.8924	271073	33.0593	33.1363
Lena	163381	36.0842	35.9258	207145	38.8967	38.8837	270761	33.1584	33.1375
Baboon	245793	30.8758	30.8848	234373	36.2935	36.2527	295745	30.4922	30.5150
Peppers	147553	38.4410	38.5882	201868	39.6997	39.6758	266333	33.8967	33.8913

5. SECURITY ANALYSIS

The knights randomize the path in the chosen block of 8×8 pixels, and then there are 64! Possible ways
In the chosen gray image of size 256×256 there are 1024 possible blocks, if the blocks are randomized then there are 1024! ways.
If DES adopted, prior to embedding, then it randomizes the data in 2^{64} possible ways.
Here n is also variable, it varies from 1 to 5 maximum
Hence the total complexity is $2^{64}\times1024! \times 64! \times 5$
From this analysis it is obvious that one has to perform $2^{64}\times1024! \times 64! \times 5$ number of attacks to crack the secret message. This security level estimation reveals the sternness of the proposed stego against hackers.

6. CONCLUSION

It is understood that the major requirements of data hiding are imperceptibility, robustness and high data capacity, and thus this methodology has been developed keeping in mind these prerequisites. Here we have employed four pixel block differencing method, along with n-bit Modified Least Significant Bit (MLSB) substitution method, Knight's tour and Re-adjustment procedure. By using n-bit Modified Least Significant Bit (MLSB) substitution method, security is enhanced, while with Knight's tour, the data embedding path is unique and very difficult to crack by eavesdroppers while the readjustment procedure gives levels of imperceptibility a high boost. Also, the picture's quality is not disrupted significantly to the human eye, by embedding adaptively into the edge pixels higher than that of the smooth pixels. Thus perceptual distortion is significantly reduced. Furthermore, this procedure also has the capacity to embed considerable payloads. Thus, in overall this technique is one that meets all requirements diligently and serves the purpose for which it is created.

REFRENCES:

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

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", *Signal Processing*, Vol. 90, 2010, pp. 727-752.

[4] C.K. Chan, L.M. Chen, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, Vol. 37, No. 3, 2004, pp. 469–474.

[5] C. Lin, Y.B. Lin, C.M. Wang, "Hiding data in spatial domain images with distortion tolerance", *Computer Standards & Interfaces*, Vol. 31, No. 2, 2009, pp. 458–464.

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

[7] C.C. Chang, H.W. Tseng, "A steganographic method for digital images using side match", *Pattern Recognition Letters*, Vol. 25, No. 12, 2004, pp. 1431–1437.

[8] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding-A Survey", *Proceedings of the IEEE, special issue on protection of multimedia content*, Vol. 87, No. 7, July 1999, pp. 1062-1078.

[9] R.Amirtharajan, Adharsh, D Vignesh, V R.John Bosco Balaguru, "PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography", *International Journal of Computer Applications,* vol. 7 No. 9, 2010, pp. 31-37.

[10] H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proceedings in Vision, Images and Signal Processing,* Vol. 152, No. 5, 2005, pp. 611–615.

[11] Y.R. Park, H.H. Kang, S.U. Shin, K.R. Kwon, "A Steganographic Scheme in Digital Images Using Information of Neighboring Pixels", *Springer-Verlag, Berlin Germany, LNCS* 3612, 2005. pp. 962–967.

[12] C.H. Yang, C.Y. Weng, A steganographic method for digital images by multipixel differencing, in: *Proceedings of International Computer Symposium*, Taipei, Taiwan, R.O.C., 2006, pp. 831–836.

[13] M.Padmaa Dr.Y.Venkataramani." ZIG-ZAG PVD - A Nontraditional Approach". *International Journal of Computer Applications,* Vol. 5, No. 7, 2010, pp. 5–10.

[14] Xin Liao, Qiao-yan Wen, 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, 2011, pp. 1-8

[15] 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 Transaction on Information Forensics Security*, Vol. 3, No. 3, 2008, pp. 488–497.

[16] Amirtharajan, R. Balaguru, R.J.B, "Tri-layer stego for enhanced security - a keyless random approach", *IEEE International Conference on Internet Multimedia Services Architecture and Applications,* Dec 2009 doi: 10.1109/IMSAA.2009.5439438

[17] R.Amirtharajan, Krishnendra Nathella and J Harish, "Info Hide – A Cluster Cover Approach" *International Journal of Computer Applications,* Vol. 3, No. 5, 2010, pp. 11–18.

[18] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", *IEEE Security Privacy Magazine*, Vol. 1, No. 3, 2003, pp. 32–44.

[19] KokSheik Wong, Xiaojun Qi, Kiyoshi Tanaka, "A DCT-based Mod4 steganographic method", *Signal Processing,* Vol. 87, No. 6, 2007, pp. 1251–1263.

[20] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering*, Vol. 4, No. 3, 2006, pp. 275-290.

[21] 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,* 2011 pp. 157 - 162 D.o.i 10.1109/ICCCET.2011.5762459

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

[23] Mordecki. E., "On the Number of Knight's Tours, "Prepublicacion es de Malem6tica de la Universidad de la Repliblica, 2001/57.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] Gordon, V. S. and T. J. Slocum, "The Knight's Tour Evolutionary vs. Depth-First Search", *IEEE Congress on Evolutionary Computation*, Vol. 2, 2004, pp. 1435-1440

[25] McKay, B. D. Knight's tours of an 8x8 chessboard, Department of Computer Science, Australian National University. 1997.

AUTHOR PROFILES:

Mr.V.Thanikaiselvan received his M.Tech degree from SASTRA University, Thanjavur, Tamilnadu, India in 2006. Now he is pursuing his Ph.D degree in VIT University in the field of Image steganography. Currently he is working as an Assistant Professor (Senior) in Communication Engineering Division under School of Electronics Engineering, VIT University, Vellore, Tamilnadu, India. His research interest includes Wavelet domain Image processing, Image Compression, Data hiding, Random Image Steganography, Graph Theory and Cryptography. He is also working as a Co-Principal Investigator, SAR Image Processing funded by DRDO, Government of India, New Delhi.

SANTOSH KUMAR was B.Tech (ECE) student (2007-2011) in VIT University, Vellore, Tamilnadu, India. Currently He is working for Cognizant Technologies-India .

NARALA NEELIMA was B.Tech (ECE) student (2007-2011) in VIT University, Vellore, Tamilnadu, India.

R. Amirtharajan was born in Thanjavur, Tamil Nadu province India, in 1975. He received B.E. degree in Electronics and Communication Engineering from P.S.G. College of Technology, Bharathiyar University, Coimbatore, India in 1997 and M.Tech. in Computer Science Engineering from SASTRA University Thanjavur, India in 2007. He joined SASTRA University, Thanjavur, Tamil Nadu, India (Previously Shanmugha College of Engineering) as a Lecturer in the Department of Electronics and Communication Engineering since 1997 and is now Assistant Professor, He is currently working towards his Ph.D. Degree in SASTRA University. His research interests include Image Processing, Information Hiding, Computer Communication and Network Security. So far he filed one International Patent; he has published 16 Research articles in National & International journals and 4 IEEE conference papers. He is Life member in CRSI India, SSI, IAENG, and IACSIT. He also served as TPC member & review member for 10 IEEE & Springer supported International Conferences apart from 3 SCI Indexed Journals. Presently he is also working on funded project in the field of Steganography supported by DRDO, Government of India, New Delhi.