Research Journal of

Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 263-276, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.263.276

Horse Communication against Harsh Attack: A Stego Ride

V. Thanikaiselvan and P. Arulmozhivarman
School of Electronics Engineering, VIT University, Vellore, Tamil Nadu, India

Corresponding Author: V. Thanikaiselvan, School of Electronics Engineering, VIT University, Vellore, Tamil Nadu, India

ABSTRACT

The common techniques used to implement image steganography are: One-Modified Least Significant Bits (LSB) substitution techniques with the readjustment procedure to reduce the Mean Square Error (MSE); Two-Pixel Indicator (PI) to increase the complexity of embedding procedure; Three-random path inside the file. These techniques, when used without making much compromise on the critical parameters, ensure enhanced security of the secret data. In this study, we propose to effectuate the knight's tour for random walk without altering the quality of the image. To ensure full security, randomization of the Red, Green and Blue (RGB) planes of the cover image using row vector is implemented and the obtained image is divided into four pixel blocks. Then, knight's tour to choose successive block follows the Pixel Value Differencing (PVD) to embed data optimally. Thus, this method assures a highly imperceptible and complex steganography with higher capacity.

Key words: Steganography, row vector scrambling, pixel indicator, modified LSB, pixel value differencing

INTRODUCTION

In the present Digital age, large amount data which mainly of comprises of picturizations of events, things, ideas are used for communication or interaction in the social media. This exchange employs both web based technologies and mobile based technologies used by organizations, communities and individuals to interact between them, marking the advancement in all the major fields (Cheddad *et al.*, 2010). While The Social Media and it forms (e-Magazine, podcats, web chats, voice, video, photos, micro blogs, Internet blogging) have gained wide publicity, they are still vulnerable especially when they contain any specifications about model designs, Patents, or any ongoing research work. To secure the integrity and authenticity of the digital media exchange Steganography (Gutub, 2010; Amirtharajan and Rayappan, 2012a, b; Amirtharajan *et al.*, 2012; Bender *et al.*, 1996) a branch of science and information security, performs secret communication with the sole aim to hide the very existence of secret information in the cover in order to circumvent any ambiguity in perception (Amirtharajan and Rayappan, 2012a, b; Chan and Chen, 2004; Chang and Tseng, 2004).

The cover file used to hide or the secret data file can be in the form of any multi-media format like image, video and audio file (Bender *et al.*, 1996; Katzenbeisser and Petitcolas, 1999). Cryptography is yet another technique used to shield a consumer data on an open medium by jumbling the data resulting in an indecipherable format which is bound to draw the attention of hackers (Schneier, 2007). A slight modification of the cover image due to embedment of the secret data in the cover results in the stego image (Chan and Chen, 2004; Chang and Tseng, 2004).

Steganography has many key objectives, which are: imperceptible secret message, withstanding capacity to several image processing methods like data compression techniques and embedding capacity of data, a distinction from its relative techniques such as watermarking and cryptography (Zanganeh and Ibrahim, 2011; Schneier, 2007; Katzenbeisser and Petitcolas, 1999).

Copyright marking techniques and steganography are the two categorizations under information hiding that have gained great momentum in the contemporary times (Cheddad *et al.*, 2010; Schneier, 2007; Huang and Fang, 2011; Janakiraman *et al.*, 2012a, b). While working on a large-scale image, preference is generally given to steganography, considering the fact that it increases the embedding capacity and image's imperceptibility (Amirtharajan and Rayappan, 2012a, b; Chan and Chen, 2004). However, copyright marking techniques centre on enhancing the grips of the protection of copyrights (Katzenbeisser and Petitcolas, 1999; Zeki *et al.*, 2011).

Additionally, there are two types that come under the steganographic methods; the first type camouflages secret data utilizing the spatial domain of a cover image, that is to say, that the secret data is concealed right into the pixels in the host image (Amirtharajan and Rayappan, 2012a, b; Amirtharajan *et al.*, 2012; Chan and Chen, 2004; Chang and Tseng, 2004; Janakiraman *et al.*, 2012a; Lin *et al.*, 2009; Liao *et al.*, 2011; Mordecki, 2001; Padmaa *et al.*, 2011; Park *et al.*, 2005; Thanikaiselvan *et al.*, 2012b; Thien and Lin, 2003; Wang *et al.*, 2001, 2008; Wu and Tsai, 2003; Wu *et al.*, 2005; Yang *et al.*, 2008). However, the second type conceals secret data by making use of transformed domain of the cover image (Amirtharajan *et al.*, 2012; Thanikaiselvan *et al.*, 2011, 2012a). Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) are few among the various transformation operations that are used to refurbish the pixel values which are in the spatial domain of the host image into coefficients in the frequency domain. Then, the coveted data is embedded in them.

The most widespread universal technique in steganography is the Least Significant Bit-LSB substitution (Amirtharajan and Rayappan, 2012a, b; Chan and Chen, 2004; Chang and Tseng, 2004; Lin *et al.*, 2009; Thien and Lin, 2003; Wang *et al.*, 2001; Yang *et al.*, 2008; Zhao and Luo, 2012; Zhu *et al.*, 2011). Here, the objected pixel in a cover image taken into consideration involves their least significant n-bits being embedded with the data bits. Moreover, not every pixel can sustain equal quantity of coveted data (Park *et al.*, 2005).

In order to develop this, suggestion on several novel consistent LSB approaches has been done (Yang *et al.*, 2008). Among these, a few involve the notion of human vision used to enhance the clarity of the stego images by hiding extra bits in edge region involving distinct curves as compared to a smooth area, since a human eye is far less perceptive to edge areas than smooth areas (Amirtharajan and Rayappan, 2012a, b; Chan and Chen, 2004; Wang *et al.*, 2001).

In information hiding, steganography features the ability to preserve the authenticity in a secret correspondence, while watermarking and Cryptographic encryption distinguishes an ownership protection and data security, respectively (Cheddad *et al.*, 2010; Katzenbeisser and Petitcolas, 1999). Proposition had been made by Chan and Cheng (2004) with regard to a simple LSB substitution in supplementary to the Optimal Pixel Adjustment Process (OPAP). However, by using the Pixel-Value Differencing (PVD) (Chang and Tseng, 2004; Liao *et al.*, 2011; Park *et al.*, 2005; Wang *et al.*, 2001, 2008; Wu and Tsai, 2003; Wu *et al.*, 2005) has proposed a unique optimized Least Significant Bit (LSB) substitution methodology which yields the higher hiding capacity along with imperceptible stego image. Moreover, Wu and Tsai (2003) have proposed a method to establish the number of coveted bits that can be embedded depending on the pixel value differencing.

A method involving four pixel blocks differencing concept with a unique LSB substitution had been proposed by Liao *et al.* (2011). An amalgam of pixel-value differencing method and a subsequent LSB substitution technique has been proposed by Wu *et al.* (2005). Bearing in mind, the least of the two difference assessments in PVD method by means of adjacent pixels, an innovative method is proposed by Park *et al.* (2005). In order to decide the number of secret data bits that can be embedded, Yang *et al.* (2008) have proposed adaptive data hiding in edge areas. The absolute value of two neighbouring pixels to conceal coveted data is used in the method proposed by Wang *et al.* (2008).

A comprehensive study on steganographic methods on digital image and for secret communication; including watermarking and encryption are also gathered by Cheddad *et al.* (2010) Several reviews on steganography and cryptography methods and implementations are available in hardware and firmware (Janakiraman *et al.*, 2012b; Rajagopalan *et al.*, 2012). Pixel Indicator based stego structure was originally proposed by Gutub (2010) and further, an exhaustive work was done by Amirtharajan and Rayappan (2012c, d) using LSB, where the secret data embedded in the Least Significant Bits (LSB) of the image pixels based on the randomization principle has been implemented by using coloured channels (Janakiraman *et al.*, 2012a; Padmaa *et al.*, 2011; Thanikaiselvan *et al.*, 2012b). Spread spectrum based steganography method (Thenmozhi *et al.*, 2012) is also another option. Kelley Seibel elicited the way knight tour's (Gordon and Slocum, 2004; Seibel, 1994; Mordecki, 2001) could be created on the Cylinder and Torus.

Distinctively scrutinizing every one of the aforementioned papers, the proposed scheme imparts a stego with a random nature and enhanced PSNR and thus, the security. The RGB planes of a colour image could be randomized using a row vector followed by the knight's tour in order to hide secret data in random fashion, thus escalating its security has been signified in this research paper.

Also that, this paper draws to the forefront, the notion behind hiding and organizing the data inside the images. In the following sections description on the proposed methodology and the experimental observations are discussed.

PROPOSED METHODOLOGY

Randomization of color plane of image: Consider 'x' number of pixels in the RGB color image. The row vector has to be divided into 'k' blocks on creation of 'x' sized row vector. Here, every p sub block is contained in block(b_i) where (p = x/k) and p is an integer.

$$b_i = i + (k \times p') \tag{1}$$

$$\text{Row vector} = [b_1\ b_2\ b_3\ b_4\ \ldots\ldots\ldots.\ b_k] \tag{2}$$

where, b_i represents ith block of row vector (1 = i = k), p' represents position of sub block in each block (0 = p' = (p-1)). Row vector is illustrated in Fig. 1. The position of pixel for exchanging R, G, B pixel values which is currently considered is indicated by row vector. Taking into account various values for k in raster scan, the pixels have to be chosen column wise, while in the host image, choice is done randomly. The image can be perceived to be like cover image with the alterations in color of image even after performing the following steps.

Figure 2a and b shows the pixel randomized image. Implementation of the randomization of the color plane of image provides high security. Each value of the row vector is divided by 3 and the following operation is to be performed on the colour plane of corresponding pixel of cover image:

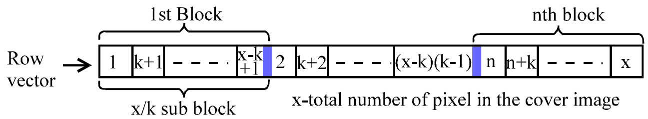

Fig. 1: The row vector to be considered for randomization of color plane of image

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

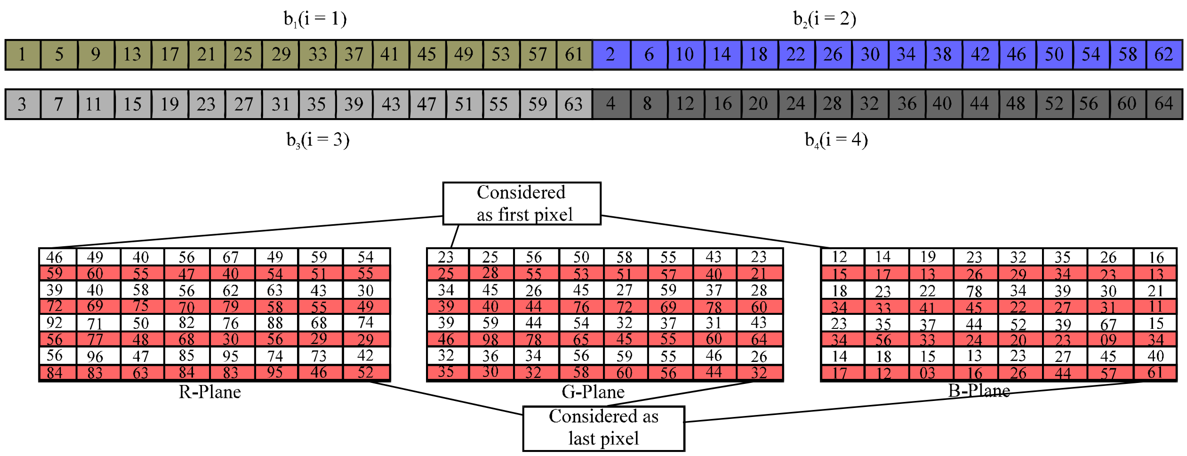

Fig. 2(c): Example of Row vector for pixel randomization

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

Example of pixel scrambling:

- bi = i + (k × p')
- Row vector = [b1 b2 b3 b4 ……… . bk]
- Let x = 64, k = 4
- p = x/k = 16
- Position of subblock (p') => 0 = p' = 15
- Row vector =[b1, b2, b3, b4]

From the Fig. 2c, first value of row vector is 1; Therefore, mod(1,3) gives 1. Now R-plane first pixel value 46 will be replaced as 23 and G-plane first pixel value will be replaced as 46. Same way all pixels can be interchanged.

Table 1: Meaning of indicator values

Bits	CHANNEL-R	CHANNEL-G
00	Next m bits of data embedded in channel R obtained by PVD	First m bits of data embedded in channel 2 obtained by PVD
01	No secret data embedding	Embed secret data of n bits
10	Embed secret data of m bits	No secret data embedding
11	First m bits of data embedded in channel R obtained by PVD	Next m bits of data embedded in channel G obtained by PVD

Pixel indicator method: Gutub (2010) had proposed stego system based Pixel Indicator. Pixel Indicator Method is used to embed secret data randomly in colour images using LSB. Random selection colour plane and number of bits to be inserted can be done by this method. Three bytes are used to represent each pixel in a colour image which gives Red, Green and Blue intensities in that pixel. This method is used to increase the security and capacity of steganography. Adaptive embedding of secret data can be done using Pixel Indicator along with PVD (Pixel Value Differencing) which improves the quality of stego image. Channel and Indicator is the colour plane of the RGB image. In Table 1, column shows the last two bits of the pixel of indicator plane and column 2 and 3 shows operation done on the pixels of that channel (colour plane).

Example for pixel indicator: A 2×2 sample is taken from Blue Plane (After scrambling) and given below:

$$v = \{46, 49, 59, 60\}$$

$$\begin{matrix} 46 & 49 \\ 59 & 60 \end{matrix}$$

First pixel is 46, then mod (46, 4) is 2 $(10)_2$, therefore, embedding will be done only in R-Plane and no data embedding in G plane.

Knight's tour: Knight's tour is marked by the journey of the knight through all the squares once in an n×n chessboard. While the last square is an invalid move to the first square by the knight in open knight's tour, in closed or the cyclic knight's tour, it is considered to be a valid move by knight. Moving one square across horizontally and two squares up or down vertically or two squares across horizontally and with one square up or down vertically, that is in ordinary words performing a move in an 'L' shape is an applicable knight move shown in Fig. 3. The first mathematical analysis of this problem statement was made by Euler in 1759. From then on, research has been made to find the possible number of knight's tours for given n×n matrix. Even till date, not all the square matrices have a knight's tour. Seibel (1994) has proposed in his research work that one can get even more probable knight tours by presuming the square matrices as cylinders and torus. This study, the square matrix as a cylinder has been utilized to embed the secret data along the knight's move. Imbibing this idea, since the search space is significantly high in steganography, high security could be attained even with the knowledge of initial square of knight's move.

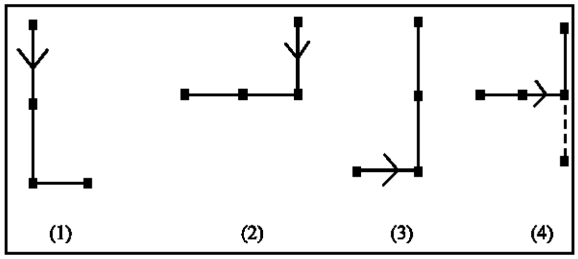

Fig. 3: Cyclic order to be followed for closed knight's tour for $n_1 \times n_2$ matrix

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. 4: Completed knight's tour on the 8×8 cylinder

Even though there are no circuits on the $n_1 \times n_2$ (n_1 and n_2 are even numbers and $n_1 = 4$) cylinder, the following is an algorithm which gives a tour for the $n_1 \times n_2$ cylinder. Start in any co-ordinate in the matrix. Then the movements as per the templates given in the Fig. 3. All movements are similar to kingts movement in the chess board. Use all the templates cyclically i.e., first 1 to 4 again 1 to 4. In the 4th template, if the upper co-ordinate is already visited then move the immediate down co-ordinate. A completed knights tour for 8×8 matrix is shown in Fig. 4.

IMPLEMENTATION

Implementing the randomization of the color plane of cover image provides for high security with the help of row vector. Without actual perception of distortion, more secret bits can be made to endure in edge area pixels as compared to the smooth areas. By m-bit Modified Least Significant Bits (MLSB) substitution, pixels in blocks of host image are concealed with coveted data bits where n is decided by considering the average difference of the block according to where it belongs-Smooth (m_l) or edge area (m_h). To depreciate the distortion even after embedding the secret data to cover image, readjustment procedure is sought, by which it is made certain that the average differenced value would be in identical level. Using knight's tour, improvement in securing the embedded secret data is done randomly in the host image. Embedding process and extraction process are elicited as follows.

Algorithm for embedding: A host image can be assumed to be a color image. Blocks of four pixels each is formed by dividing the cover image which does not overlap one another. For each block taken into consideration, four pixels $x_{i,j}$, $x_{i,j+1}$, $x_{i+1,j}$, $x_{i+1,j+1}$ would be considered with their gray values to be v_o, v_1, v_2 and v_3, respectively. The following are the exhaustive steps in embedding procedure:

Step 1: Noting the number of pixels of host image in a color plane, create an equivalent row vector of size say (x). Each of the k blocks obtained on division, p sub blocks (p = x/k where, p is an integer) is contained in bi blocks:

$$b_i = i + (k \times p') \text{ and Row vector} = [b_1\ b_2\ b_3\ b_4 \ldots\ldots\ldots.\ b_k]$$

Here, ith block of row vector is denoted by b_i (1 = i = k). Also, position of sub block of every block is represented by p'. (0 = p' = (p-1)):

Step 2: Every element has to be divided by 3 in a row vector

- If 0 is obtained as a reminder, no alterations have to be made in a colour plane
- If 1 is obtained reminder, R and G plane pixel value has to be exchanged
- If 2 is obtained reminder, the following has to be done

R plane pixel has to be replaced with B plane pixel, similarly G plane pixel with R plane pixel, B plane pixel with G plane pixel value. This has to be repeated for all pixels of a colour plane of cover image:

Step 3: Each of the colour planes of the cover image has to be divided into blocks of non overlapping four pixels value (2×2)

Step 4: The chosen four pixel block has to be used for embedding by providing the position of starting square of knight's tour by using knight's path

Step 5: Component of blue plane of the starting pixel of chosen block has to be divided as in previous step by 4. (Pixel Indicator):

- If 0 is obtained as reminder, the operation in steps 5-10 have to be performed firstly on R-plane and then on G-plane
- If 1 is obtained as reminder, the operations explained in step 5-10 have to be performed on G-plane
- If 2 is obtained as reminder, the operations explained in step 5-10 have to be performed on R-plane
- If 3 is obtained as reminder, the operation in steps 5-10 have to be performed firstly on G-plane and then on R-plane

Step 6: The average of differencing value Ä has to be calculated, which is given by:

$$\Delta = \frac{1}{3}\sum_{i=0}^{a} v_i - v_{min} \quad (3)$$

Here, v_0, v_1, v_2, v_3 are the pixel values and the mínimum is given by $v_{min} = \min\{v_0, v_1, v_2, v_3\}$:

Step 7: In our proposed methodology, using two levels (lower level and higher-level), the concealment of messages constructively is carried out. Having obtained $\Delta \le T_h$, Δ belongs to "lower-level" or in other words this block pertains to smooth area and m is found to be equal to m_l. If not, Δ pertains to "higher-level" or in other words, the block is a part of an edge area where $m = m_h$, satisfying the criteria: $2^{ml} = T_h = 2^{mh}$ and $1 = m_l$, $m_h = 5$

Step 8: The block is verified if it belongs to "Error Block" or not. In case it does not, next step has to be continued. Else, restart the process from Step 4

ERROR BLOCK

The block is known as the "Error Block" if and only if $\Delta \le T_h$ and $v_{max} - v_{min} > 2\times T_h + 2$ where, $v_{max} = \max\{v_0, v1, v2, v3\}$ is assumed. For example, let block be (216, 217, 216, 230) and $T_h = 5$ pertains to "Error Block", since 230-216 = 14>2×5+2 = 12.

Step 9: By embedding 'm' message bits in the LSB of each of the four pixels, v_i is converted to v_i'

Step 10: The m-bit modified LSB substitution technique has to be applied to v_i', and let v_i" be the denotation of the result (0 = i = 3)

Step 11: "Readjusting procedure" is the name given to this step. Assume, $vc_i = v_i'' + l \times 2^n$, ($0 \le i \le 3$), $l \in \{0,1,-1\}$ and (vc_0, vc_1, vc_2, vc_3) has to be hunted for, such that:

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

- I. Δ and Δ conform to identical level, where $vc_{min} = \min\{vc_0, vc_1, vc_2, vc_3\}$
- II. The stego block finally obtained-(vc_0, vc_1, vc_2, vc_3) are not a part of the "Error Block"
- III. Depreciation of value of

$$\sum_{k=0}^{3} \{(vc)_i - v_i\}^2$$

[MSE] is carried out

After (vc_0, vc_1, vc_2, vc_3) has replaced (v_0, v_1, v_2, v_3) in each of the block, Repetition of Steps 4-10 has to be carried out until each of the blocks of cover image is covered.

Step 12: Step-1 is repeated once again in order to obtain final stego image

Example of LSB Embedding:

- Let T_h=21, m_l = 2 and m_h = 4 (user Defined)
- If $\Delta > T_h$, $m = m_h$, else $m = m_l$
- vmin = min{46 49 59 60} = 46
- Δ = (0+3+13+14)/3 = 10
- m= m_l = 2
- Let the message bits are {11 01 11 10}
- After LSB Embedding v' = {47, 49, 59, 62}
- v" is obtained by optimum pixel adjustment process[9]

Extraction algorithm: Stego image provides for direct extraction of the coveted bits. Divide the final stego image into four pixel block which are non-overlapping for extraction as is done in the embedding scheme. Assume the four neighboring pixels to be v_0, v_1, v_2 and v_3. The following steps are utilized to extract the secret data:

Step 1: The operations noted in step-1 to 4 in algorithm for embedding have to be performed

Step 2: Component of blue plane of the starting pixel of the block has to be divided by 4. If reminder is 0, no extraction is done, 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 than on R-plane

Step 3: The average difference value Δ has to be found out

Step 4: The order of level in which Ä lies has to be found out by using the threshold (T_h) value. Having obtained Δ, if it lies in the lower level or smooth area, $m = m_l$, else if it belongs to higher level or edge area, $m = m_h$

Step 5: The block has to be validated for error. If it is a part of the error block, move to the step 2 or else move on to next step which is step 6

Step 6: From, m bit LSB of pixels (0 = i = 3), extraction of the 4 m secret bits is performed

Step 7: Next block from which the secret data has to be retrieved using Knight's Tour is to be chosen and yet again, on the 2×2 block, steps 2-6 have to be performed in order to retrieve the embedded message

Step 8: Until every block is sequenced to extract the entire coveted data, repeat the process

RESULTS AND DISCUSSION

In order to decide upon the performance characteristics of our proposed methodology, several experiments have been carried out. Color images sized 256×256 are taken into consideration with a figure of seven as cover images, which are depicted in Fig. 5. In our proposed methodology, consideration of 2×2 blocks that are distinctly separate from one another is done along with the edge features, which is the edge area pixels that sustain enhanced alterations having minimal visual distortion. A text of larger volume considered as the secret data is transformed into the digital format which is marked by ones and zeroes. They are then embedded into the cover image that serves as a host. In order to evaluate the superiority of the stego image, Peak Signal to Noise Ratio (PSNR) is calculated which is defined by the following for an M×N grayscale image.

$$\text{PSNR} = 10\log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P_{i,j} - q_{i,j})^2} \tag{5}$$

Here, $p_{i,j}$ and $q_{i,j}$ represent the pixels in cover image and the final stego image, respectively. The stego images with various values of T_h, m_l and m_h are illustrated in Fig. 6-11. Data

Fig. 5(a-g): Cover images of size 256×256×3; (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master and (g) Ubuntu

Fig. 6(a-g): Stego images (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master and (g) Ubuntu for $T_h = 7$, $m_l = 2$ and $m_h = 3$

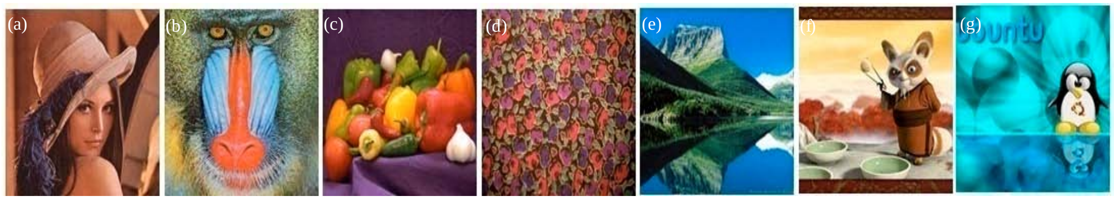

Fig. 7(a-g): Stego images (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master, (g) Ubuntu for $T_h = 12$, $m_l = 2$ and $m_h = 4$

Fig. 8(a-g): Stego images (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master,(g) Ubuntu for $T_h = 15$, $m_l = 3$ and $m_h = 4$

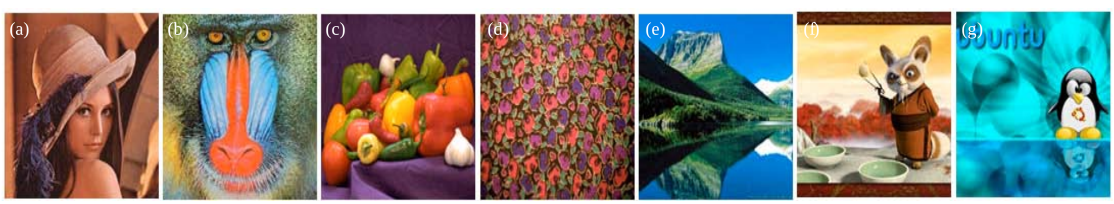

Fig. 9(a-g): Stego images (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master and (g) Ubuntu for $T_h = 18$, $m_l = 2$ and $m_h = 5$

Fig. 10(a-g): Stego images (a) Lena, (b) baboon, (c) peppers, (d) fabric, (e) Hills, (f) Master and(g) Ubuntu for $T_h = 18$, $m_l = 3$ and $m_h = 4$

Fig. 11(a-g): Stego images (a) Lena, (b) Baboon, (c) Peppers, (d) Fabric, (e) Hills, (f) Master and (g) Ubuntu for $T_h = 21$, $m_l = 4$ and $m_h = 5$

hiding in these numerals are bound to alterations. However, they are certainly indiscernible to naked human eye, which proves that the proposed method has significantly surmounted distortions that result from concealing secret data with high capacity. We have experimented with numerous values of m_l, m_h and threshold.

Taking, for example, T_h = 12, 2-4 by performing division with Δ, if the block conforms to average difference value (Δ) with a value lower than threshold level, then 2 bit-secret message bits are hidden in each pixel of the chosen block. Else if average difference value (Δ) is greater than the threshold level, then 4 bits of secret data is embedded through modified LSB substitution in all the pixels. Table 2 and 3 shows the results of all the cover images. Capacity will be decided by the size of the cover image, for example, if the cover image size is 512×512 instead of 256×256 cover image, then the capacity will also be 4 times greater and the PSNR remains same.

In addition, randomizing colour channels through row vector and knight's tour prior to embedding will offer high security and high embedding capacity. Table 4 shows the comparative study of secret data embedding with Liao *et al.* (2011) method and our technique. The present method shows high capacity embedding as well as better preservation of PSNR in the stego images.

STEGANALYSIS

The technique of detecting and extracting the secret data from the stego image is known as steganalysis. In this proposed algorithm, the minimum PSNR is 38 dB for T_h = 15 and T_h = 18, except at T_h = 21, which implies that the algorithm is imperceptible by the eye, "Human visual Attack".

Table 2: PSNR and capacity of proposed algorithm with different T_h and m_l and m_h

	T_h = 7, m_l = 2 and m_h = 3		T_h = 12, m_l = 2 and m_h = 4		T_h = 15, m_l = 3 and m_h = 4	
Cover image	Capacity (bits)	Avg. PSNR (dB)	Capacity (bits)	Avg. PSNR (dB)	Capacity (bits)	Avg. PSNR (dB)
Lena	291865	44.22	377033	38.56	379901	38.58
Baboon	292233	44.17	380361	38.38	381701	38.38
Papers	294657	44.29	385897	38.46	389789	38.47
Fabric	293485	44.2	385817	38.34	385621	38.36
Hills	280101	45.05	354889	39.31	370221	39.15
Master	291381	44.31	373441	38.66	379249	38.7
Ubuntu	290895	45.12	383785	39.27	389213	39.27

Table 3: PSNR and capacity of proposed algorithm with different T_h and m_l and m_h

	T_h = 18, m_l = 2 and m_h = 5		T_h = 18, m_l = 3 and m_h = 4		T_h = 21, m_l = 4 and m_h = 5	
Cover image	Capacity (bits)	Capacity (bits)	Capacity (bits)	Avg. PSNR	Capacity (bits)	Avg. PSNR
Lena	442793	442793	375845	38.74	469425	32.90
Baboon	449153	449153	377237	38.36	469577	32.64
Papers	469649	469649	387737	38.48	480633	32.46
Fabric	460917	460917	381317	38.42	474425	32.56
Hills	417217	417217	366321	39.22	458693	33.42
Master	435653	435653	374697	38.86	467361	33.08
Ubuntu	475745	475745	388845	39.23	486581	33.31

Table 4: Comparative results (T_h = 15, m_l = 3 and m_h = 4) (T_h = 18, m_l = 3 and m_h = 4)

	Liao *et al.* (2011)		Proposed method		Liao *et al.* (2011)		Proposed method	
Cover (256×256)	Capacity (bits)	Avg. PSNR	Capacity (bits)	Avg. PSNR	Capacity (bits)	Avg. PSNR	Capacity (bits)	Avg. PSNR
Lena	144801	39.12	379901	38.58	205749	37.45	375845	38.74
Baboon	206293	32.57	381701	38.38	246497	32.27	377237	38.36
Papers	142207	39.84	389789	38.47	204008	37.89	387737	38.48

To avoid the secret data from being detected from the stego image, the embedding procedure is carried out in the spatial domain in a highly randomized fashion, fortifying it from the Blind Steganalysis technique also. In case of an attempt to hack the information from a 256×256 pixel image, the assailant will have to iterate the technique an exhaustive number of times before obtaining the information as the following security schemes have been implemented.

- Pixel scrambling
- Pixel indicator
- Knight's tour
- Adaptive bit embedding

Liao *et al.* (2011) in his algorithm has adapted this technique for grayscale images but no security measures were added. But, in this proposed technique the RGB image is activated with four security schemes to achieve multilevel security using color image steganography method.

CONCLUSION

An optimized method in steganography has been exemplified on the basis of amalgam four-pixel block differencing along with the modified LSB substitution and knight's tour. Modified LSB substitution as well as readjustment procedure has been employed by which the mean square error has depreciated. For enhancing the safety of secret data hidden in a cover media, random walk within the file has been implemented by knight's tour for random walk, thereby quality image remaining intact. We employ pixel indicator method of embedding in order to secure the communication and randomization of the three planes of RGB host image is also carried out with row vector. In our proposed method, results establish that higher security with high embedding capacity has been provided in addition to superior quality of the image. In steganography, robustness to various image processing schemes, the embedding capacity, and last but not the least, the imperceptivity constitute a paranormal triangle. It is implied that the robustness would be forsaken in smaller proportion with high embedding capacity (e.g., 486581 bits) along with fine image quality (33.11 dB).

REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inf. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inf. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inf. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inf. Technol. J., 11: 566-576.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recogn. Soc., 37: 469-474.

Chang, C.C. and H.W. Tseng, 2004. Steganographic method for digital images using side match. Pattern Recognition Lett., 25: 1431-1437.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Gordon, V.S. and T.J. Slocum, 2004. The knight's tour evolutionary vs. depth-first search. Proceedings of the Congress on Evolutionary Computation, Volume 2, June 19-23, 2004, Sacramento, CA., USA., pp: 1435-1440.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 56-64.

Huang, H.C. and W.C. Fang, 2011. Techniques and applications of intelligent multimedia data hiding. Telecommun. Syst., 44: 241-251.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inf. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inf. Technol. J., 11: 9-19.

Katzenbeisser, S. and F.A.P. Petitcolas, 1999. Information Hiding Techniques for Steganography and Digital Watermarking. 1st Edn., Artech Print, Canton Street Norwood, MA., ISBN-13: 978-1580530354, pp: 220.

Liao, X., Q.Y. Wen and J. Zhang, 2011. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J. Vis. Commun. Image Represent., 22: 1-8.

Lin, I.C., Y.B. Lin and C.M. Wang, 2009. Hiding data in spatial domain images with distortion tolerance. Comput. Standards Interfaces, 31: 458-464.

Mordecki. E., 2001. On the Number of Knight's Tours. Pre-Publicaciones de Matematica de la Universidad de la Republica, Uruguay.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inf. Technol. J., 10: 1896-1907.

Park, Y.R., H.H. Kang, S.U. Shin and K.R. Kwon, 2005. A steganographic scheme in digital images using information of neighboring pixels. Adv. Natural Comput., 3612: 962-967.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Seibel, K., 1994. The knight's tour on the cylinder and torus. Department of Mathematics, Oregon State University.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012a. Horse riding and hiding in image for data guarding. Procedia Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inf. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recog., 36: 2875-2881.

Wang, C.M., N.I. Wu, C.S. Tsai and M.S. Hwang, 2008. A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Software, 81: 150-158.

Wang, R.Z., C.F. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognit., 34: 671-683.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Wu, H.C., N.I. Wu, C.S. Tsai and M.S. Hwang, 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proc. IEEE Vision Image Signal, 152: 611-615.

Yang, C.H., C.Y. Weng, S.J. Wang and H.M. Sun, 2008. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Secur., 3: 488-497.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inf. Technol. J., 10: 1285-1294.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inf. Technol. J., 10: 1367-1373.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inf. Technol. J., 11: 209-216.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inf. Technol. J., 10: 1983-1988.