Tech Science Press

Scrambling Based Riffle Shift on Stego-Image to Channelize the Ensured Data

R. Bala Krishnan[1], M. M. Anishin Raj[2], N. Rajesh Kumar[1], B. Karthikeyan[3], G. Manikandan[3,*] and N. R. Raajan[4]

[1]Department of CSE, SASTRA Deemed University, Kumbakonam, India
[2]Department of CSE, Viswajyothi College of Engineering and Technology, Kerala, India
[3]School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, 613401, India
[4]School of Electrical and Electronics Engineering, SASTRA Deemed University, Thanjavur, India
*Corresponding Author: G. Manikandan. Email: manikandan@it.sastra.edu

Abstract: In recent years information hiding has got much attention as it acts as an alternate option for secured communication. The Secret content would get imbedded with the image using various possible image embodiment techniques, in which the Least Significant Bit (LSB) substitution is one of the preferred content embodiment strategy; however, asserting the quality and the originality of the content embedded image (stego) is yet a grievous concern in the field of Information Security. In this article, a proficient Scrambling Based Haar Wavelet Transform (SBHWT) approach has been sought to ensure the novelty of the stego-image that supports the safe transfer of data over the channel. In this process, the image is scrambled using a Sudoku pattern, and then streams of the secret content are embedded into the image blocks based on the proposals of the Bishop Traversal logic of chess. The content embodiment is attempted using normal LSB substitution and DNA pattern based substitution. Next, the image is descrambled to recover the original image, which is then subjected to Haar wavelet transformation for image resolution reduction. The resultant reduced image is channelized to the recipient and the inverse action of the SBHWT is made in order to get back the secret code stream. The experimental results demonstrate that the projected SBHWT approach is less predictable and exclusive in its pattern.

Keywords: Wavelet transform; bishop tour; content concealment; LSB embedding; secret data; scrambling

1 Introduction

The fortification of private content has become a primary concern in the field of information security as a result of recent developments in digital communication. 'Stego' and 'Crypto' are two terms used to describe two techniques for encrypting and hiding images' content [1]. In order to apportion the secret content, information concealment techniques like steganography are required, and steganography involves hiding secret content in images, audio, video so that eavesdroppers cannot detect the presence of the hidden secret code [2,3] and the practice of hiding the content in an image or an audio or a video file is known as "Content Embedding" procedure [4–6].

Furthermore, the growth of steganography makes it a valuable method for protecting secret information over the internet. This practice leads to better image (stego) analysis capabilities [7,8] that are associated with dissimilar content embedding [9,10] schemes. Various steganographic methods are discussed [11–25]. Frequency [26] and spatial [27] are the two major categories. The classification is done on the basis of their domain on input (cover) images. In domain converters such as DCT and DWT, the secret contents are hidden in the transformed coefficients of the input image. The encrypted secret code is masked by applying LSB, run-length, PVD, reversible, mod and lossless schemes in the spatial domain. Random and raster scan schemes are to be utilized in the LSB based content embedding procedure to hide the secret code in the pixels of the image. Raster scanning is preferred to random scanning due to the difficulty of extracting content from the image.

The Optimal Pixel Adjustment Process (OPAP) is used by Chan et al. to increase the value of content embedded images using plain LSB substitution. Pixel adjustment strategy, which accumulates the count based on the neighboring pixels, will determine the number of bits embedded in each of the image pixels. Yang et al. present a LSB substitution strategy that uses a raster scan method to improve stego-images. This practice involves processing the secret code before the content is embedded. Raghupathy et al. [28] present an efficient method of embedding content using the Bishop Tour principle of chess game in which the content embodiment could be realized by following the black and white bishop tour principle. Provos et al. have proposed a random way approach to select the image pels for secret code embedding. One content embedding practice using random fashion has been described by Tuomas Aura, which uses Secured Hash Algorithm (SHA) logic and stego key to create unique pels locations for secret content embedding procedures. By following the pattern of Queen positioning in an 8×8 chessboard, Manikandan et al. [29] present another LSB with Queen tour based embedding scheme.

In this proposed paper, the authors propose and demonstrate a novel method for image scrambling and wavelet transformation, as well as a Bishop tour practice based on chess game for embedding content. During the illegal content extraction, the work has been imposed in order to achieve massive complexity and greater payload. The projected design consists of two different touring schemes, namely, the Black-Bishop Tour and the White-Bishop Tour. For k-bit Normal (NLSB) and DNA pattern LSB (DPLSB) embedding, all of the above approaches are considered. Using a Sudoku pattern, the cover image is separated into equal numbers of smaller blocks before embedding the secret data. During the secret code embedding practice, the tour patterns have been implemented for content embedding in each block, then the image gets descrambled to obtain the order of original image; this tour pattern implementation, which results in the least mean square error and maximum Peak Signal to Noise Ratio (PSNR) value for those blocks. The generated stego image will not significantly change the input image and it would not be visible to the naked eye [30] and the stego image is then resized by applying the Haar transformation. A fine tour of each block is identified, as well as a descrambling pattern and reconstruction matrix for stego image resizing. The pattern of each tour pattern, as well as the descrambling Sudoku code and reconstruction matrix, were taped and kept as a secret (key) in order to help with content extraction.

2 Related Works

In recent years, numerous research studies have been conducted in the area of Sudoku solver and Steganography. Varieties of strategies have also been suggested on Steganography and Sudoku solver and are employed for data concealment on images that provides lossless image enciphering techniques.

2.1 Image Scrambling with Sudoku Pattern

By using Sudoku patterns and Latin squares, an image scrambling approach is presented by Yue Wu et al. and Zhang et al. [31–33]. The Shuffling and Sudoku patterns are used to scramble the image, and

the reverse Sudoku and Shuffling pattern is needed for descrambling the image to recover the original. As the name suggests, Sudoku denotes to a puzzle grounded on numbers; typically, it comprises of a 9-by-9 grid which is divided into nine 3 × 3 sub-blocks. A subset of 'M' × 'M' matrices of Sudoku puzzle are perimetrically generated [34].

2.2 Steganography with Wavelet

A new approach for improving data security by aggregating stream and block ciphers has been stated by Manikandan et al. [35]. The aim of this proposed research plan is imbed the secret content in a scrambled image and make it descrambled, which is then subjected to size reduction procedure without the loss of content. For the purpose, the proposed plan proceeds with wavelet transformation principle. The wavelet transformation [36,37], which is characterized by translation and dilation factors to get over the Fourier transforms. An approach using Gabor compression is stated by Mythreyi et al. [38]. In this article Steganography is attained on images using Gabor Transform and the scheme is denoted as Gabor Transform Based Image Steganography. Another Steganography pattern is proposed by Po-Yueh, et al. for content embedding in frequency domain. This works on the basis of users need on the embedding capability and image quality. Apart from the domain space practices, the DWT implementation results in the secret message embedding on the high frequency coefficients and the low frequency sub-bands are preserved without alteration to enhance the quality of the image. Random Number Generator (RNG) is to be used for content embedding on image, in which the RNG works to obtain the pixel locations [39]. In domain Steganography, wavelets are covered to attain information concealment. Here at the closing stage of content hiding practice, content are transformed into Discrete Haar Wavelet Transform (DHWT) coefficients which are easily decomposed into signals and images. In the phase of reconstruction inverse DHWT (IDWHT) need to be followed to obtain the lossless stego image [40,41].

Several cases of wavelets, such as Daubechies, Biorthogonal, Coiflet, Symlet, Haar [42–45], morelet and maxican-hat wavelets are available, among which Haar Wavelet is virtually the lightest wavelet in its form.

2.3 The Characteristics of Haar Wavelet

The transformation and its inverse of an image grants identical values to input image by means of a set of weighted basis functions, then the transformation is believed to encompass perfect reconstruction and it guarantees best performance in terms of its computational time. The magnitude response of the filter should be accurately zero exterior to the occurrence range roofed by the transform and the input image is separated into parts of high and low frequency and this can be enabled by means of filters.

3 Proposed System

For the implementation of the proposed SBHWT technique, five different images with resolution 'm' × 'n', where n = m for square image, have been taken as inputs and are stated in the Fig. 1i–1v.
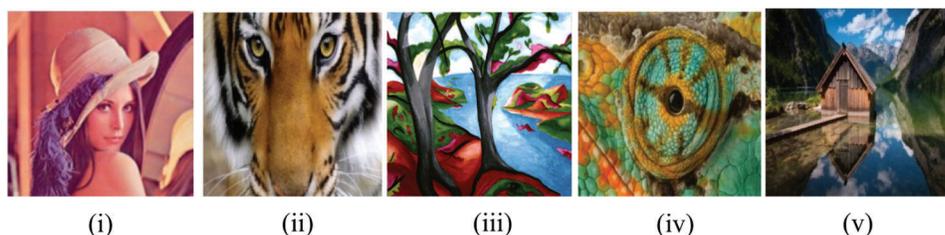

(i)　　(ii)　　(iii)　　(iv)　　(v)

Figure 1: Input images for SBHWT technique implementation (i) Lena (ii) Tiger (iii) Tree (iv) Eye (v) Nature

The implementation of the suggested approach starts with image segmentation, in which the cover image is sub divided into blocks of equal size as required for Sudoku based scrambling process. The resolution of the cover image at the beginning of the process was 540×540, the next level the image can be subdivided into nine 180×180 blocks, each of which is then subdivided into nine 60×60 blocks and at the next level it is subdivided into nine 20×20 blocks. The main theme of the proposed scheme (SBHWT) is to perform the scrambling process on the image using Sudoku pattern and hence the input image with resolution 540×540 has been considered, through which the sub blocks could be created effectively over the multiples of three.

Now the image is exposed to the scrambling process by applying the Sudoku pattern. This can be accomplished by considering each individual blocks as Sudoku game cells and by applying the Sudoku puzzle answer on the blocks. The input image is now scrambled and the key for descrambling the image is the Sudoku puzzle. Fig. 2 states the implementation of a Sudoku pattern on image 'Lena (Fig. 1i) and its corresponding output. The next level of proposed implementation is the secret content imbedding process by the LSB substitution principle.
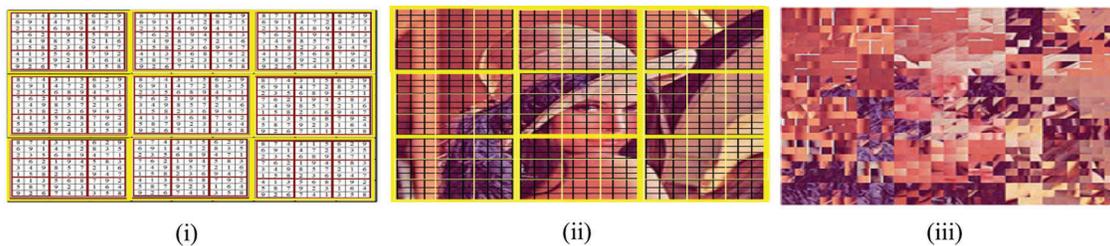

(i)   (ii)   (iii)

Figure 2: Sudoku pattern, cover image and its corresponding scrambled image (i) Sudoku pattern (ii) Cover image (iii) Scrambled image

The pixel (pel) selection for the LSB substitution proceeds with the Bishop Tour principle of Chess game in an 8×8 block and its corresponding pixel selection path is stated in the Fig. 3. The LSB substitution technique implants the secret code in the NLSB and DPLSB substitution fashion, which is stated in the Fig. 4.
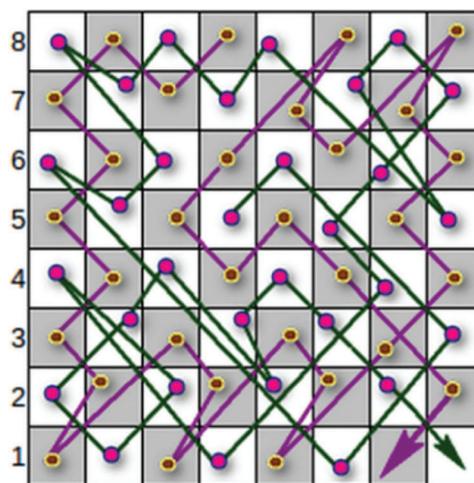

Figure 3: Pel accessing order of bishop (White & black bishop traversal)
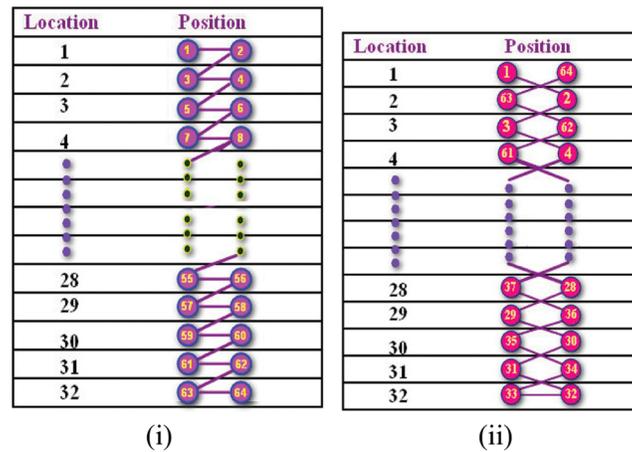
Figure 4: Normal LSB substitution and DNA structure based LSB substitution (i) Normal LSB (NLSB) substitution (ii) DNA pattern LSB (DPLSB) substitution

3.1 Fashions Behind the Substitution

NLSB substitution works by embedding the secret stream content in the LSB locations 2 and 1 of every pel location on the image. The first two bit from the secret stream gets embedded on the first pel location and the next two bit of the stream on the second pel location and the procedure gets completed after embedding the entire secret code stream and the pattern is stated in Fig. 4i.

DPLSB substitution works by embedding the secret stream content in the alternate LSB locations. The first two bit of the secret stream content gets embedded in the LSB position 2 and 1 on the first and second pel location, the next two bits in the LSB position 2 and 1 on the third and fourth pel locations and the practice is continued up to the embodiment of stream in the LSB position 2 and 1 on the pel locations 'n − 1' and 'n'. After reaching the pel location 'n' the embodiment procedure works in the reverse order by embedding 'n + 1' and 'n + 2' stream bits on the LSB position 1 and 2 on the pel location 'n' and 'n − 1' and the practice gets over after reaching the starting pel location. The execution practice of this DPLSB is stated in Fig. 4ii.

Traditional techniques of the Steganography work by embedding the content on the normal images but in the proposed method the content embedding procedure is applied on the scrambled image and it gets descrambled after the embodiment. Hence through the proposed approach multi levels of security gets obtained for the secret code stream through the scrambling with embedding and transformation procedure. The first level of security is the scrambling procedure and the next level is the content substitution pattern. The proposed SBHWT approach offers third level of security by reducing the resolution of the image by applying Haar transformation technique. The transformation performs the resolution reduction over the image in lossless fashion and through this transformation the image of resolution 'm' × 'm' gets reduced to 'm/2' × 'm/2' and the reduced images are transferred over the communication channel. The constraint for the applying the transformation is that the resolution value (m) must be a positive even value, so that the image gets reduced in to its exact half.

The content extraction at the receiver end needs to perform the reverse transformation procedure along with exact scrambling and LSB extraction procedure to obtain the original secret code stream. The algorithm for the proposed SBHWT approach for content embedding is stated in Section 3.2.

3.2 Algorithm: Scrambling Based Haar Wavelet Transform (SBHWT) Approach for Content Embedding

Inputs:

i) Cover Image (CI)

ii) Sudoku Pattern (SP)

iii) Secret Code Stream (SCS)

iv) Reduction level (RL)

v) Substitution method (SM) (i.e, SM = NLSB or DPLSB)

vi) TRAVERSAL_SCHEME (i.e, BISHOP_TRAVERSAL)

Outputs:

i) Key for image resizing (KEY_IR) and Content Extraction Scheme(CES)

CES= TRAVERSAL_SCHEME + SM

ii) Reduced Image (RI)

Step-1: Identify the Secret Code Stream (SCS) for Embedding practice.

Step-2: Identify the Cover Image (CI) and Sudoku Pattern.

Step-3: Calculate the Size of SCS and store it in 'S' for deciding the pels for embedding.

Step-4: Fragment the cover image in to 'M' equal size blocks (CI_1, CI_2,…. CI_M)

    and call SCRAMBLING process.

Step-5: SCRAMBLING

     begin

for Blocks= 1 to M

 /*Apply Sudoku Pattern to all the image blocks*/

         CI(Blocks) = Sudoku_Pattern(CI(Blocks))

       end for

    end begin

Step-6: Combine the Scrambled blocks (CI_1, CI_2,…. CI_M) to obtain Scrambled Image (SI).

Step-7: Apply Substitution method (SM) on SI using input Secret Code Stream (SCS).

    begin

      SI=SI + TRAVERSAL_SCHEME(SM(SCS));

    end begin

Step-8: Apply DE-SCRAMBLING procedure on SI to obtain $\overline{SI}$

    i.e.   SI = CI + SP;

(Continued)

(continued)

$$\overline{SI} = SI + INVERSE\_SP$$

Step-9: Apply Haar Transformation (RL) to obtain Reduced Image (RI)

    begin;   counter = 1;

        while (count < RL)

            for cols = 1 to max_rows ($\overline{SI}$)

                for rows = 1 to max_cols($\overline{SI}$)

            $\overline{SI} = \overline{SI}$ + Apply COLUMN reduction procedure of Haar Transform

                /* Intermediate values for Reconstruction phase*/

                      KEY_IR = KEY_IR + KEY($\overline{SI}$);

            end for

        $\overline{SI} = \overline{SI}$ + Apply ROW reduction procedure of Haar Transform

            /*Intermediate values for Reconstruction phase*/

                KEY_IR = KEY_IR+ KEY($\overline{SI}$);

        end for

        count = count + 1; /* Increment 'count' value by 1*/

      end while

    RI = $\overline{SI}$; /* Final Size reduced image is named as Reduced Image (RI)*/

    end begin

Step-10: Transmit the RI over the channel to the recipient and share the KEY_IR and CES.

    The proposed Scrambling Based Haar Wavelet Transform approach holds the execution procedure of Haar wavelet transformation principle for the image resolution reduction practice [41] along with the Sudoku based scrambling scheme to increase the level of security over the confidential content, which is embedded over the images. The SBHWT approach receives the inputs as Cover Image, Sudoku pattern, Secret code stream, Reduction level, Substitution scheme and Traversal procedure. The Sudoku pattern is applied on the Cover image in order to generate the scrambled image for which the image is initially sub divided in to equal size blocks. The substitution scheme is either NLSB or DPLSB substitution scheme and its procedure is stated in the Fig. 4. The Sudoku pattern is applied to the cover image in order to generate the scrambled image for which the image is initially subdivided into equal size blocks. It is either the NLSB or DPLSB substitution scheme, and its procedure is shown in Fig. 4. The sudoku pattern is applied to the image blocks and as a result, a scrambled image is created, in which the secret code stream is embedded by following the Bishop Tour traversal scheme, as illustrated in Fig. 3, which locates the pels over the image. Information is embedded in the scrambled image, and the image is then put through to the descrambling process to obtain the original image. The image is then subjected to haar wavelet transformation for resolution reduction, in which the column reduction and row reduction processes are carried out by joining the neighboring pels at row-wise and at column-wise to generate a reduced image with half the original resolution.

The content extraction procedure of SBHWT approach receives the inputs as Reduced Image, Sudoku pattern, Reduction level and Content extraction scheme. The received image needs to be reconstructed to get back the original image with its resolution value, which serves as the base to apply the Sudoku pattern on it to obtain the secret code stream.

The block diagram for the projected methodology (SBHWT) and the image scrambling strategy are stated in the Figs. 5 and 6. In the sender side the cover image is subjected to scrambling procedure using the Secret pattern key and the secret code is embedded on the scrambled image to obtain the stego image, which is then subjected to descrambling to obtain the original form of the image. The scrambling practice follows the mathematical Sudoku logic, in which the images gets separated into same size blocks and are then subjected to Sudoku pattern scrambling to obtain the reordered image and the execution procedure is stated in Fig. 6.
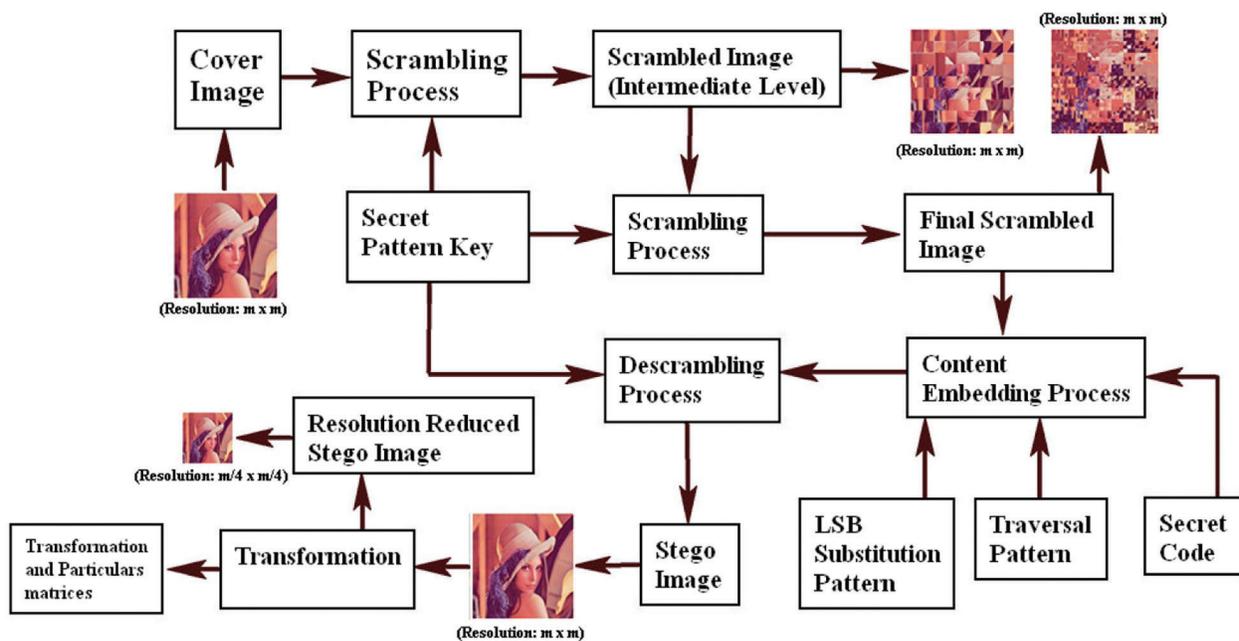

Figure 5: Block diagram of scrambling based wavelet transform (SBHWT) approach

After the descrambled image (stego image) is transformed by the Haar Wavelet Transform (HWT), it is parted into four frequency bands. LL, LH, HL, and HH are the four frequency bands. The initial band (LL) corresponds to the input stego image, which is filtered with a Low Pass Filter (LPF). LPF reduces the size of the input image by half. The remaining bands are referred to as 'particulars or details' (LH, HL, and HH), to which the High Pass Filter (HPF) is applied. In particular, the second band contains chars of vertical direction, the third band contains chars of horizontal direction, and the final band (HH) represents the characteristics of diagonal direction of the input stego image. Because the input images used for this analysis are combinations of two dimensions, wavelet transformation is performed twice in each dimension. It is initially performed row-by-row and then column-by-column.

With each stage, the filter (high pass) generates information of 'particulars'; while the filter (low pass) paired with scaling function results in coarse 'estimates'. The 'estimation' (2-level LL band) is sent following the successful decomposition of the stego image. Receiver reconstructs the original size of the stego image using Inverse Haar Wavelet Transform (IHWT) with the help of 'particulars' bands. Figs. 7 and 8 depict the block diagram for 4-band wavelet decomposition and its corresponding configuration for 2-level decomposition.
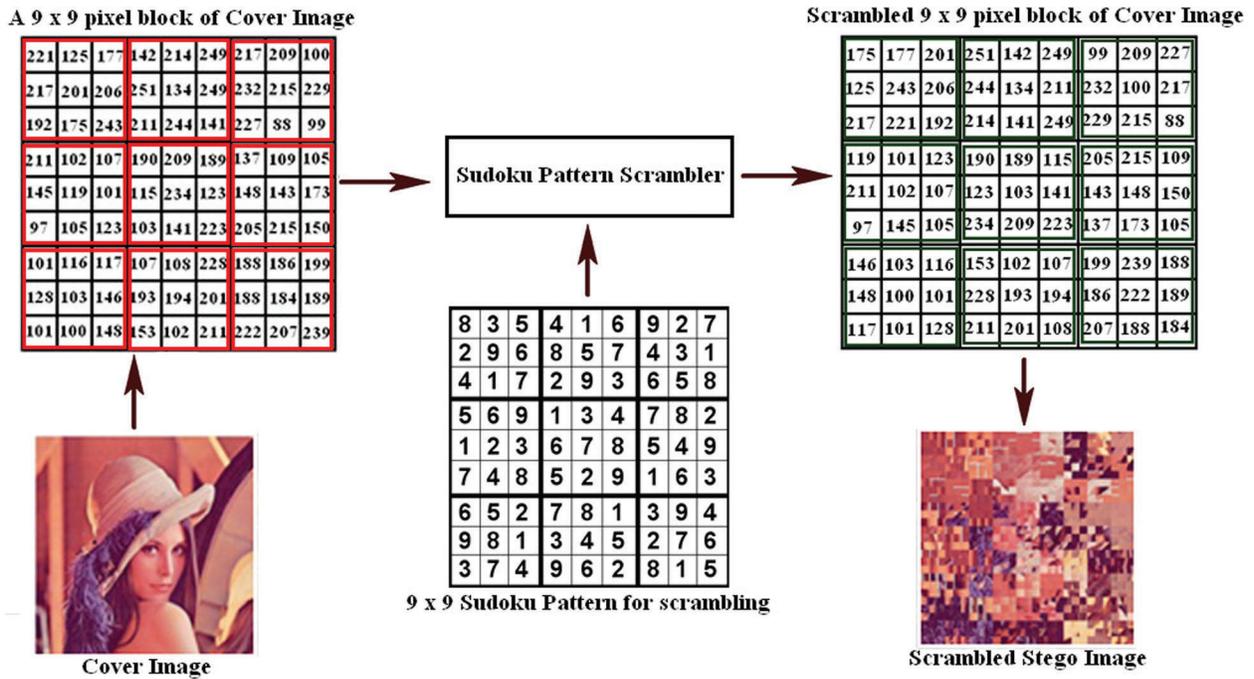
Figure 6: Sudoku based image scrambling procedure

Figure 7: Sudoku pattern-1 (P-1)

After the successful reconstruction, the secret code gets extracted from the image by applying Sudoku pattern and traversal scheme with substitution process. Then the Sudoku pattern is applied on the image to obtain the scramble image on which the bishop traversal scheme is followed with NLSB or DPLSB scheme for extracting the secret code stream.

8	9	3	5	6	2	7	1	4
7	6	4	3	9	1	2	8	5
1	5	2	4	8	7	9	3	6
2	1	7	6	3	4	5	9	8
5	4	8	2	7	9	3	6	1
6	3	9	1	5	8	4	7	2
3	2	1	7	4	6	8	5	9
9	7	6	8	2	5	1	4	3
4	8	5	9	1	3	6	7	2

Figure 8: Sudoku pattern-2 (P-2)

4 Experimental Observations

In digital image processing, several metrics are used to measure different properties of images. In order to measure the quality of images and the error rate between them, PSNR and MSE are used. A nearly inverse relationship exists between the two. Additionally, other methods like compression ratio, content embedding and extraction time play a significant role in image processing.

SBHWT has been realized in MATLAB and tests are conducted using the color images in Fig. 1. Initially, the image blocks would be scrambled using the Sudoku pattern. Tabs. 1 and 2 shows the sample cover image, stego image and respective resolution reduced images.

The proposed approach has been tested by applying two different Sudoku patterns 'P-1' and 'P-2', which are stated in Figs. 7 and 8. The MSE and PSNR values are calculated on cover image, scrambled image along with time of execution were shown in Tabs. 3 and 4.

From the Tabs. 3 and 4, it is evident that the input cover image is having significant difference with the scrambled image over both the patterns P-1 and P-2 and the creation time of scrambled image depends on the pattern.

5 Implication of the Proposed Approach

The proposed SBHWT method consists of three different techniques for assessing the content confidentiality. They are

- Image scrambling and de-scrambling.
- Secret Code embedding technique using Bishop traversal for locating the pels and LSB substitution gets implemented as NLSB or DPLSB.
- Image decomposition and its corresponding reconstruction using Discrete Haar wavelet transform and its Inverse.

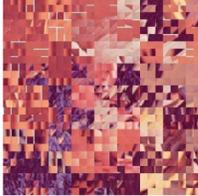**Table 1:** Cover images and their respective stego images

Cover Image	Scrambled Image	Stego Image with Bishop Traversal based NLSB Substitution	Stego Image with Bishop Traversal based DPLSB Substitution

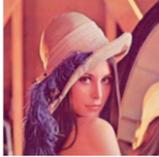**Table 2:** Stego images and their respective resolution reduced images

Stego Image with resolution 540 x 540	Transformed Stego Image with resolution 270 x 270	Transformed Stego Image with resolution 135 x 135

Table 3: MSE and PSNR comparison of cover image and P-1 applied scrambled image

Cover image	Scrambled image						Execution time (seconds)
	MSE			PSNR			
	Red	Green	Blue	Red	Green	Blue	
Lena	4210.549	3970.061	3745.058	11.887	12.142	12.396	16.01
Tiger	2443.159	2707.441	2440.422	14.251	13.805	14.256	15.05
Tree	10802.976	9795.237	8052.365	7.795	8.221	9.072	15.04
Eye	7159.873	4665.476	4025.319	9.582	11.442	12.083	16.04
Nature	4626.475	3327.971	3944.877	11.478	12.909	12.170	15.01

Table 4: MSE and PSNR comparison of cover image and P-2 applied scrambled image

Cover image	Scrambled image						Execution time (seconds)
	MSE			PSNR			
	Red	Green	Blue	Red	Green	Blue	
Lena	3752.653	3457.081	3161.707	12.387	12.744	13.132	15.55
Tiger	2536.817	2804.874	2513.948	14.088	132.652	14.127	14.97
Tree	11173.214	10310.778	8549.530	7.649	7.998	8.811	16.00
Eye	7607.128	4331.964	3618.124	9.319	11.764	12.546	14.01
Nature	4625.856	3119.671	3426.226	11.479	13.190	12.770	16.05

In the normal steganographic approaches the pels accessing order needs to be known to extract the content but the proposed approach hold the first lock at image reconstruction at the receiver end; the second lock at the image scrambling process and then final complicated lock on the pels accessing order, which is the Bishop traversal logic and the content extraction approach is either NLSB pattern or DPLSB logic.

6 Conclusion

The projected SBHWT approach offers an efficient scheme for pels identification in an image for content embedding and its extraction process. The LSB substitution scheme gets utilized with a modified version named DPLSB, which embeds the data in DNA pattern over the image, which would be the added effect over the stego principles. The image scrambling holds the lock on the image which needs to open to extract the content from the image. The significant feature of the proposed approach is that the image resolution reduction procedure which forms an additional lock on the secret content helps the network channel with fewer payloads as compared with the original image. At the receiver side, the image can be precisely recreated and the secret content is extracted without any degradation of quality. From the experimental outcomes, it is apparent that the proposed scheme proves to be a reliable methodology for information concealment over images. This research work could focus on video data in the future.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Bruice, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed., India: John Wiley, 2007.

[2] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz et al., "Applications for data hiding," *IBM Systems Journal*, vol. 39, no. 3&4, pp. 547–568, 2000.

[3] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3&4, pp. 313–336, 1996.

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

[5] F. A. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding–A survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[6] S. Katzenbeisser and F. A. Petitcolas, "Information hiding techniques for steganography and digital watermarking," in *Artech House Computer Security Series*, 1st ed., Norwood, MA, USA: Artech House, 2000.

[7] L. Qingzhong, H. S. Andrew, Q. Mengyu, C. Zhongxue and R. Bernardete, "An improved approach to steganalysis of JPEG images," *Information Sciences*, vol. 180, pp. 643–655, 2010.

[8] T. Zhang, W. Li, Y. Zhang, E. Zheng and X. Ping, "Steganalysis of LSB matching based on statistical modeling of pixel difference distributions," *Information Sciences*, vol. 180, no. 23, pp. 4685–4694, 2010.

[9] A. Westfeld, "Space filling curves in steganalysis," in *Proc. SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII*, San Jose, California, USA, pp. 28–37, 2005.

[10] X. Luo, D. Wang, P. Wang and F. Liu, "A review on blind detection for image steganography," *Signal Processing*, vol. 88, no. 9, pp. 2138–2157, 2008.

[11] C. Chang, T. Chen and L. Chung, "A steganographic method based upon JPEG and quantization table modification," *Information Sciences*, vol. 141, no. 1-2, pp. 123–138, 2002.

[12] C. Chang, W. Wu and Y. Chen, "Joint coding and embedding techniques for multimedia images," *Information Sciences*, vol. 178, no. 18, pp. 3543–3556, 2008.

[13] C. Chang, P. Pai, C. Yeh and Y. Chan, "A high payload frequency-based reversible image hiding method," *Information Sciences*, vol. 180, no. 11, pp. 2286–2298, 2010.

[14] C. Chang, C. Lin and Y. Wang, "New image steganographic methods using run-length approach," *Information Sciences*, vol. 176, no. 22, pp. 3393–3408, 2006.

[15] P. Chen and H. Lin, "A DWT based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.

[16] C. Chang and T. D. Kieu, "A reversible data hiding scheme using complementary embedding strategy," *Information Sciences*, vol. 180, no. 16, pp. 3045–3058, 2010.

[17] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 11, pp. 2875–2881, 2003.

[18] C. Chang, C. Lin and Y. Fan, "Lossless data hiding for color images based on block truncation coding," *Pattern Recognition*, vol. 41, no. 7, pp. 2347–2357, 2008.

[19] R. Z. Wang, C. F. Lin and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2000.

[20] T. Aura, "Practical invisibility in digital communication," in *Proc. Workshop on Information Hiding, Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, vol. 1174, pp. 265–278, 1996.

[21] C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function," *Journal of System and Software*, vol. 81, no. 1, pp. 150–158, 2008.

[22] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm," *Information Sciences*, vol. 177, no. 15, pp. 3099–3109, 2007.

[23] F. Zhang, Z. Pan, K. Cao, F. Zheng and F. Wu, "The upper and lower bounds of the information-hiding capacity of digital images," *Information Sciences*, vol. 178, no. 14–15, pp. 2950–2959, 2008.

[24] Y. R. Park, H. H. Kang, S. U. Shin and K. R. Kwon, "An image steganography using pixel characteristics," in *Proc. CIS*, China, pp. 581–588, 2005.

[25] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognition*, vol. 41, no. 8, pp. 2674–2683, 2008.

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

[27] H. Sagan, "Space-Filling Curves," in *Universitext*. New York: Springer-Verlag, 1994.

[28] B. Raghupathy, R. Namachivayam and N. Raajan, "An enhanced bishop tour scheme for information hiding," *International Journal of Applied Engineering Research*, vol. 9, pp. 145–151, 2014.

[29] G. Manikandan, R. Bala Krishnan, R. Varadharajan and G. Dharshini, "An 8-queen algorithm based steganographic approach for secure key exchange," *International Journal of Applied Engineering Research*, vol. 9, no. 7, pp. 763–769, 2014.

[30] N. Johnson, Z. Duric and S. Jajodi, "Information hiding: Steganography and watermarking: Attacks and countermeasures," in *Advances in Information Security*, 3rd ed., USA: Springer, 2003.

[31] Y. Wu, Y. Zhou, J. P. Noonan and S. Agaian, "Design of image cipher using latin squares," *Information Sciences*, vol. 264, no. 11, pp. 317–339, 2014.

[32] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 12, pp. 2775–2780, 2011.

[33] Y. Y. Wu, S. Agaian and J. P. Noonan, "Sudoku associated two dimensional bijections for image scrambling," *Information Sciences,* vol. 327, pp. 91–109, 2012.

[34] Y. Y. Wu, Y. Zhou, J. P. Noonan, K. Panetta and S. Agaian, "Image encryption using the Sudoku matrix," in *Proc. SPIE 7708, Mobile Multimedia/Image Processing, Security, and Applications*, Orlando, Florida, United States, 2010.

[35] G. Manikandan, G. Krishnan and N. Sairam, "A unified block and stream cipher based file encryption," *Journal of Global Research in Computer Science*, vol. 2, no. 7, pp. 53–57, 2011.

[36] I. Daubechies, *Ten lectures on wavelets*. Philadelphia, PA: Society for Industrial and Applied Mathematics, 1992.

[37] S. G. Wallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 11, no. 7, pp. 674–693, 1989.

[38] S. Mythreyi and V. Vaidehi, "Gabor transform based image steganography," *IETE Journal of Research*, vol. 53, no. 2, pp. 103–112, 2007.

[39] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letter*, vol. 31, no. 5, pp. 347–354, 2010.

[40] D. Bloisi and L. Iocchi, "Image based Steganography and cryptography," *Computer Vision Theory and Applications*, vol. 1, pp. 127–134, 2007.

[41] G. Manikandan, M. Kamarasan and N. Sairam, "A new approach for secure data transfer based on wavelet transform," *International Journal of Network Security*, vol. 15, no. 1, pp. 88–94, 2013.

[42] I. Daubechies, "The wavelet Transform, time frequency localization and signal analysis," *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 961–1005, 1990.

[43] L. Driskell, "Wavelet-based steganography," *Cryptologia*, vol. 28, no. 2, pp. 157–174, 2004.

[44] C. Shremmer, "Decomposition strategies for wavelet based image coding," *Int. Symp. on Signal Processing and its Applications*, vol. 2, pp. 529–532, 2001.

[45] M. Vetterli and J. Kovaˇcevi, *Wavelets and Subband Coding*, 1st ed., Englewood Cliffs, New Jersey: Prentice Hall, 1995.