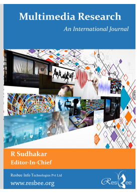
Vol. 2 No.2 April 2019

Multimedia Research

Received 11 December, Revised 7 February, Accepted 7 March



Secret Image Sharing and Steganography Using Haar Wavelet Transform

Vinusha S
Department of Applied Electronics,
Regional Centre of Anna University Tirunelveli, Tamil Nadu, India
s.vinu89@gmail.com

Abstract: Image steganography enables secure communication whether even intimating the enemy regarding the occurrence of communication. Steganography and cryptography play a vast role in rendering effective security for the secret data. However, when the presence of the secret message is revealed then, the secret message is disclosed, which is the major drawback of the existing strategies. Thus, the paper proposes an effective image sharing and steganography method using the Haar wavelet. There are two phases in this research: encoding and decoding phase. In the first phase, the encoding phase, where the secret message is embedded in the input image using the proposed Haar wavelet-based steganography, while in the decoding phase, the secret message is uncovered. In the decoding phase, the Lagrange's interpolation is applied that decodes the secret message from the stego or embedded image. The great significance of the method is that the greater degree of security is rendered against the security attacks and is a robust strategy for combining the secret sharing of messages and steganography. The analysis of the proposed method with respect to the existing methods is enabled using the 500 stego images acquired from the UCID database. The comparative analysis of the proposed method based on the metrics, such as Peak Signal-To-Noise Ratio (PSNR) and Structural Similarity (SSIM) index reveals that the proposed method acquired a maximal PSNR and SSIM of 57.142 dB and 0.9991, respectively.

Keywords: Image steganography, secret sharing, wavelet transform, Haar wavelet, UCID database

1. Introduction

In today's modern high-tech world, the Image Steganography has many applications. Privacy and anonymity is a concern for most people on the internet. Image Steganography permits for two parties to communicate secretly and covertly. It permits for some morally-conscious people to safely whistle blow on internal actions; it permits for copyright protection on digital files exploiting the message as a digital watermark. One of the other major exploits for Image Steganography is for the transportation of high-level or top-secret documents among international governments. When Image Steganography has many legitimate uses, it can also be quite nefarious. It can be exploited by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on cover operations to communicate secretly and safely.

The development of the World Wide Web and the advancement in the digital world attracted the researchers towards data hiding in the digital media [1]. One of the interesting topics in the digital revolution is the image steganography, where the secret message is hidden in the image, which is referred to as the cover image. In contrast to steganography, cryptography is a technique that renders security to the media without any data hiding but using keeps away the eavesdroppers from understanding the data. In the conventional methods, the security of the data is enabled through the application of the cryptography algorithm prior to the steganography methods so that the security of the data is assured [9]. However, there is a chance for the disclosure of the secret data. Among so many of the cryptography algorithms, secret sharing is one of the major algorithms reported in the literature. When the data is shared with only one participant then, there is a chance for data leakage instead if the secret is shared with multiple participants; there is a chance e of enhanced security. Hence, we step in the secret sharing criterion, where the data is shared with the multiple participants [10] [11].

In this paper, the secret image sharing and steganography are facilitated using the Haar wavelet, where initially, the encoding phase commences. In the first phase, the secret message is embedded in the

https://doi.org/10.46253/j.mr.v2i2.a4

image based on the Haar wavelet transform and at the decoding phase, the secret message is extracted using the inverse Haar wavelet-based steganography. In this context, the security of the communication is assured and the quality of the embedded image is assured. Following is the contribution of the research: Haar wavelet is applied to the image in the process of encoding the secret message in the cover image such that the security for the secret data is revealed.

The rest of the paper is organized as a review of the existing methods in section 2 and section 3 presents the step-wise description of the image steganography methods. The results of the method are deliberated in section 4 and finally, section 5 concludes the paper.

2. Literature Review

In this section, the review of the existing steganography methods is presented with the merits and demerits of the methods, which stood as a motivation behind developing a new method for enabling secure communication. Yang et al. [8] developed a method that recovered a secret image without any corruption and in addition, it could a counterfeit stego image with a considerable probability. Noopa Jagadeesh et al. [6] developed a steganography method based on (t,n)-threshold that rather concealed the shadows of the intruders as a higher degree of security. However, the method failed in case of the color images. Alexandre Santos Brandao and David Calhau Jorge [7] developed a method that transmitted the information efficiently and securely.

The analysis of the existing methods reveals that there are few challenges shown below: quality of the image is a major challenge that needs to be addressed and in addition, the secure communication lacks in case of the color image, and hence, there is a need for a robust method to render secure communication. In the cryptography-based approach, it is reported that the existing methods in cryptography for assuring security faces a huge problem when the presence of the secret message in the image is found as the secret message could be uncovered, which is the major challenge that seeks the need for an effective image steganography method.

3. Proposed Method of Secret Sharing and Extraction as a Mark of Secure Communication

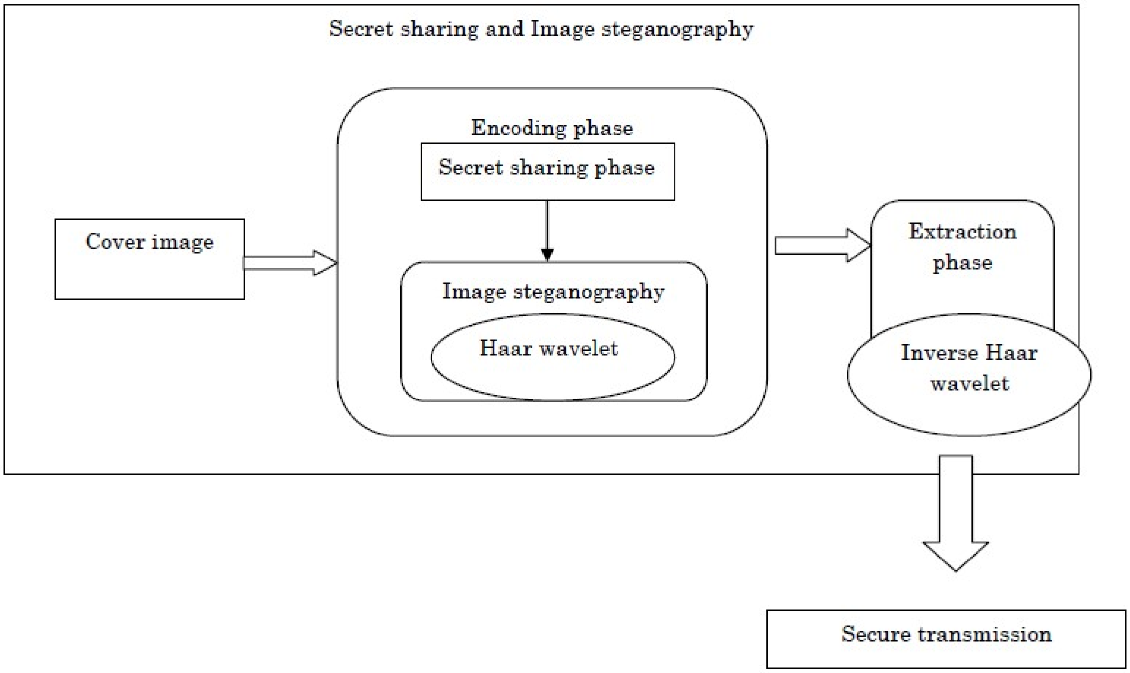


Fig. 1: *Block diagram of image steganography using Haar wavelet transform*

Image steganography is performed along with the secret sharing phenomenon to render data security. Initially, the data is shared with t number of participants and then, subjected to the image steganography process in which the Haar transform is applied. Once the shared data is embedded in the cover image using a Haar transform, the hidden data is extracted at the receiver end using the inverse

Haar transform. The Haar transform is used for image processing and pattern recognition. Hence, two dimensional signal processing is an area of effectual applications of Haar transforms because of their wavelet– like structure. Fig. 1 shows the block diagram of the proposed Haar wavelet-based image steganography.

3.1 Secret Sharing

The secret sharing is a significant phenomenon performed prior to the image steganography process. The formula that represents the secret sharing phenomenon is given by,

$$X(d)=\left\{m_0+m_1 d^1+\ldots+m_{t-1} d^{t-1}\right\} \bmod A \tag{1}$$

The above Eq. presents that the t-pixels of the secret image is put into m_0 to m_{t-1} coefficients. For each of the t pixels available in the secret image, the Eq. (1) is established followed with the generation of f shares, where the decimal amount of 5 MSB corresponding to the first pixel of f different cover images accomplish the value of d. Thus, each share comprises of the streams of X. Normally, secret sharing is performed both in visual and non-visual forms and in this research, the non-visual form is referred. Eq. (1) represents the non-visual secret sharing, termed as (d,X) secret sharing, where X specifies the total participants and d dignifies the minimal number of the participants needed for revealing the secret image.

3.2 Image Steganography using Haar Wavelet Transform

The image steganography is performed using the F16 checksum and Haar wavelet transform [14], where initially the Haar wavelet transform and F16 checksum [15] are described and the proposed steps follow:

Haar wavelet transforms: Generally, wavelet transform is the one that transforms the image between the spatial and the frequency domains and here, the wavelet concept is the one describing the waves that fade with respect to the time. Mostly, wavelet transforms to find a vast number of applications in the areas of image de-noising, smoothening, speech recognition, and so on. It is peculiar that the wavelet transform is applied to the image steganography at the point of rendering the capacity and robustness. One of the significant wavelets transforms is Haar wavelets that transform the image from the spatial to the frequency domain through a series of horizontal and vertical operations [12] [13]. The Haar wavelet employs the square pulses to approximate the original function, where the cover image is represented as low-low, low-high, high-low, and high-high, respectively, and these bands reveal the approximate, horizontal, vertical, and diagonal coefficients, respectively. It is significant to note that the approximate bands are not considered for hiding the secret messages as the human eyes are very sensitive in determining the changes in the particular band. On the other hand, the other bands contain significant information and the data could be hidden in the high-frequency bands. For the generation of these four bands, the image is scanned vertically and horizontally. Initially, the horizontal operation is insisted, where the image is split as low and high-frequency bands, which are further split as high and low-frequency bands to yield the combination of four sub-bands. Upon the completion of the embedding process, the hidden data is extracted back from the embedded image. The Haar wavelet transform comprises of the decomposition and reconstruction algorithms, which render higher security abilities to the image. The decomposition of wavelets is represented as,

$$P(k,l)=\frac{a(2k-1,2l-1)+a(2k-1,2l)+a(2k,2l-1)+a(2k,2l)}{2} \tag{2}$$

$$Q(k,l)=\frac{a(2k-1,2l-1)+a(2k-1,2l)-a(2k,2l-1)-a(2k,2l)}{2} \tag{3}$$

$$R(k,l)=\frac{a(2k-1,2l-1)-a(2k-1,2l)+a(2k,2l-1)-a(2k,2l)}{2} \tag{4}$$

$$S(k,l)=\frac{a(2k-1,2l-1) \quad a(2k-1,2l) \quad a(2k,2l-1)+a(2k,2l)}{2} \tag{5}$$

where, (k,l) symbolizes the orientation scale.

F16 checksum algorithm [15]: This is the checksum algorithm, which keeps in record two sums. One is the running sum of data in 8-bit chunks, while the other is the running sum of individual bytes multiplied using the position from an end of the data. Thus, the position details are incorporated in the checksum that protects the data against the movement in a data stream. Finally, the two sums are combined together to form the 16-bit checksums and the purpose of using this algorithm is to enable the security counterfeit.

Steganography algorithm [16]: In general, the data hiding is prevalent such that the data is less sensitive for human interpretation. The steps followed during image steganography are as follows:

- ✓ Decomposition of the cover image as frequency blocks using the Haar transform.
- ✓ Sub-divide each of the frequency as non-overlapping blocks of size $[8\times8]$, $[4\times4]$ and $[2\times2]$, respectively, where the approximate block is neglected as it is suspected to disclose the secret message and hence, it is kept away from embedding.
- ✓ Compute the visual weight for the coefficient blocks. The visual weight of the individual block corresponds to the average value of the weight with respect to the single block in order to take into account the human visual system.

Thus, in the proposed method, the shared data is hidden in the first level blocks of the wavelet corresponding to the cover image, while the checksums of the shared data are embedded in the second level blocks of the wavelet. It is significant to know the bit capacity of the individual blocks for embedding and extraction of the secret image. For the data-hiding in the cover image, the following are the limitations to be verified.

- If bit capacity B is zero, jumps to the next block.
- If $B=1$, the first eight numbers present in the shared data is hidden in the LSB of the corresponding block of the cover image. On the other hand, the F16 checksum is computed and the 16bits generated by the algorithm is filled in the LSB of the coefficients corresponding to the relative second block available in the first tree of the relevant block.
- When $B>1$ then, the steps are iterated, where eight number of share data is taken into account at the individual iteration.

Once all the share data is hidden in the cover image, the extraction phase commences.

3.3 Extraction of the Hidden Secret Message from the Stego Image

This step represents the decoding phase, where the shared data is extracted from the cover image for rebuilding the secret message from the share data. Thus, for the data extraction, inverse Haar is applied. Following are the Eq. representing the application of the inverse Haar transform.

$$a(2k-1,2l-1)=\frac{P(k,l)+Q(k,l)+R(k,l)+S(k,l)}{2} \tag{6}$$

$$a(2k-1,2l)=\frac{P(k,l)+Q(k,l)-R(k,l)-S(k,l)}{2} \quad \text{`} \tag{7}$$

$$a(2k,2l\quad 1)=\frac{P(k,l)-Q(k,l)+R(k,l)-S(k,l)}{2} \tag{8}$$

$$a(2k,2l)=\frac{P(k,l)-Q(k,l)-R(k,l)+S(k,l)}{2} \tag{9}$$

4. Results and Discussions

The results and analysis of the proposed steganography method using the Haar wavelet are presented in this section and the analysis is progressed based on the performance measures that validate the quality of the embedded image.

4.1 Experimental Setup

The implementation is performed in the MATLAB R2011a tool for which the input images are acquired from the UCID data base [5] that comprises of the 1338 uncompressed RGB images, which are the grayscale images in their respective sizes. In this research, for analysis purpose, we consider the image sizes, $[64\times64]$, $[128\times128]$ and $[256\times256]$, respectively. As a secret image, Fletcher-16 (F16) image is considered, which is later converted to $[512x512]$. Moreover, 500 stego images are considered from the databases for analysis and hence, the image quality measures, such as PSNR and SSIM are considered for analysis.

4.2 Performance Metrics

The metrics used for the comparison include PSNR and SSIM that defines the quality of the embedded image. PSNR measures the similarity between the original image and the embedded image and the method that affords with the maximal value of PSNR is reported as an effective method. PSNR is computed as,

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{\mathrm{Max}_I}{\sqrt{\mathrm{MSE}}}\right) \tag{10}$$

$$\mathrm{MSE} = \frac{1}{p * q}\sum_{i=0}^{p\ \ 1}\sum_{j=0}^{q\ \ 1}\left\|I(i,j)\quad I^*(i,j)\right\|^2 \tag{11}$$

Where, $I(i,j)$ refers to the original image and $I^*(i,j)$ symbolizes the embedded image. p and q specifies to the total number of the rows and columns in the image and Max_I dignifies the maximal signal value. MSE is the mean square computed as the mean square of the distance between the original and the embedded images. The measure SSIM between two images is computed as,

$$\mathrm{SSIM}(i,j) = \frac{(2\mu_i\mu_j + s_1)(2\sigma_{ij} + s_2)}{(\mu_i^2 + \mu_j^2 + s_1)(\sigma_i^2 + \sigma_j^2 + s_2)} \tag{12}$$

where, μ_i and μ_j refers to the mean of the total rows and columns in the image, whereas σ_i^2 and σ_j^2 refers to the variance of the total rows and columns in the image. s_1 And s_2 are the variables used for stabilizing purpose. The covariance of i and j is denoted as, σ_{ij}.The effective method reports with the maximal value of the PSNR and SSIM measure that symbolizes that the image quality is high.

4.3 Comparative Methods

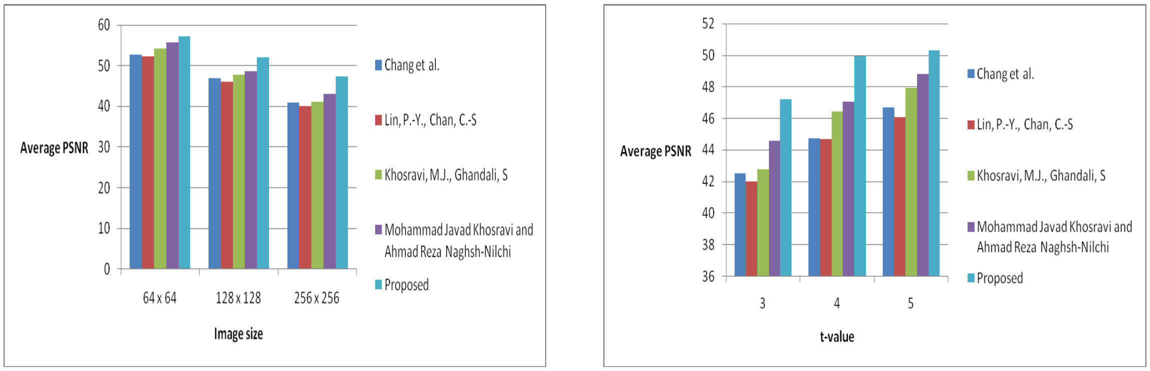
The methods used for the comparative analysis are analyzed based on the performance measures and the methods used for comparison are developed by, Chang et al. [1], Lin P Y, Chang. C. S [2], Khosravi MJ., Ghandali S [3], and Mohammad Javad Khosravi and Ahmad Reza Naghsg-Nilchi [4].

4.4 Comparative Analysis

The analysis of the methods based on varying the image size and t-value are deliberated in this section. In this section, the performance metrics are analyzed with respect to the image size and t-value (participant) such that the quality of the image is interpreted.

4.4.1 Analysis based on the PSNR by varying the image sizes: The analysis performed based on PSNR is depicted in fig. 2. Fig. 2 a) deliberates the analysis with respect to the average PSNR through varying the size of the image. When the image size is $[64\times64]$, the average PSNR is 52.72 dB, 52.19 dB, 54.32 dB, 55.65 dB, and 57.142 dB, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When the image size is $[128\times128]$, the average PSNR is 46.83 dB, 46.11 dB, 47.72 dB, 48.67 dB, and 52.16 dB, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When the image size is $[256\times256]$, the average PSNR is 40.88 dB, 39.99 dB, 41.19 dB, 43.11 dB, and 47.325 dB, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method.

The analysis performed based on PSNR [17] is depicted in fig. 2. Fig. 2 b) deliberates the analysis with respect to the average PSNR through varying the values of t. When $t = 3$, the average PSNR is 42.5 dB, 41.98 dB, 42.78 dB, 44.56 dB, and 47.213 dB, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When $t = 4$, the average PSNR is 44.71 dB, 44.65 dB, 46.45 dB, 47.07 dB, and 49.91 dB, respectively for the methods developed by Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When $t = 5$, the average PSNR is 46.67 dB, 46.04 dB, 47.9 dB, 48.81 dB, and 50.32 dB, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method.

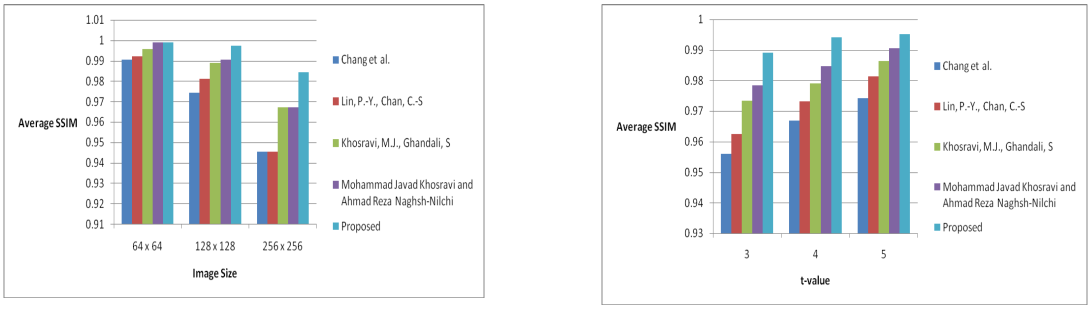


a) b)

Fig. 2. *Comparative analysis based on average PSNR, a) varying the image size, b) varying the t-value*

The analysis performed based on SSIM [18] is depicted in fig. 3. Fig. 3 a) deliberates the analysis with respect to the average SSIM through varying the size of the image. When the image size is $[64\times 64]$, the average SSIM is 0.9905, 0.9921, 0.9956, 0.9989, and 0.9991, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When the image size is $[128\times 128]$, the average SSIM is 0.9744, 0.9812, 0.9889, 0.9906, and 0.9974, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When the image size is $[256\times 256]$, the average SSIM is 0.9454, 0.9454, 0.9673, 0.9673, and 0.9845, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method.

The analysis performed based on average SSIM is depicted in fig. 3. Fig. 3 b) deliberates the analysis with respect to the average SSIM through varying the values of t. When $t=3$, the average SSIM is 0.9559, 0.9624, 0.9733, 0.9785, and 0.9891, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When $t=4$, the average SSIM is 0.9668, 0.9731, 0.9791, 0.9848, and 0.9941, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method. When $t=5$, the average SSIM is 0.9743, 0.9814, 0.9864, 0.9906, and 0.9951, respectively for the methods developed in Chang et al., Lin P Y, Chang. C. S, Khosravi MJ., Ghandali S, Mohammad Javad Khosravi, and Ahmad Reza Naghsg-Nilchi, and the proposed method.



a) b)

Fig. 3. *Comparative analysis based on average SSIM, a) varying the image size, b) varying the t-value*

It is evident from the fig.s 2 and 3 that the average PSNR and SSIM increase with the increasing values of t and the image sizes. Even though the existing methods contributed individually with the effective performance, the proposed method outperforms the existing methods with a good value for PSNR and SSIM, which are the measures that define the quality of the embedded image.

5. Conclusion

Secure communication in the digital era is the basic need in the current situation and is enabled through the peculiar technique termed as image steganography, where the media is the image. The secret image is shared with multiple participants instead of sharing with a single participant as a mark of enhancing the security of the data or secret image or any other media. Then, the image steganography is initiated using the Haar wavelet transform, which hides the data in a particular location such that the hidden data is secure. Finally, the data is transmitted and at the receiving end, the stego image is subjected to extraction of the secret message using the inverse Haar wavelet. The analysis of the method is enabled using the data acquired from the UCID database from which nearly 500 stego images are considered for analysis. The analysis is made with respect to the quality dependent parameters, such as PSNR and SSIM, which are maximal of 57.142 dB and 0.9991, respectively for the proposed image steganography scheme. The extension of the research is based on any of the optimizations that optimally locate the region to embed the secret message so that the security degree is increased further.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Chang, C.C., Hsieh, Y.P., Lin, C.H., “Sharing secrets in stego images with authentication”, Pattern. Recogn, Vol. 41, No. 10, pp. 3130–3137,2008.

[2] Lin, P.-Y., Chan, C.-S. “Invertible secret image sharing with steganography. Pattern. Recognition Letters”, Vol. 31, No. 13, pp. 1887–1893, 2010,

[3] Khosravi, M.J., Ghandali, S., “A secure joint wavelet based steganography and secret sharing method”, 7th International Conference on Information Assurance and Security (IAS), pp. 222–227, 2011.

[4] Mohammad Javad Khosravi and Ahmad Reza Naghsh-Nilchi, "A novel joint secret image sharing and robust steganography method using wavelet", Multimedia Systems,Vol. 20, pp. 215–226, 2014.

[5] Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P., “Image quality assessment: from error visibility to structural similarity”, IEEE Trans. Imag. Process Vol. 13, pp. 600–612, 2004.

[6] Noopa Jagadeesh, Aishwarya Nandakumar, P. Harmya, and S.S. Anju, " Secret Image Sharing Using Steganography with Different Cover Images", ACC 2011, Part II, CCIS 191, pp. 490–497, 2011.

[7] Alexandre Santos Brandao ; David Calhau Jorge, "Artificial Neural Networks Applied to Image Steganography", IEEE Latin America Transactions, vol.14 , no.3, pp.1361 - 1366, 2016.

[8] Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C., “Improvements of image sharing with steganography and authentication”, J. Syst.Softw. Vol. 80, No. 7, pp. 1070–1076, 2007.

[9] Provos, N., Honeyman, P., “Hide and seek: an introduction to steganography”, IEEE. Secur. Priv. Mag, Vol. 1, No. 3, pp. 32–44, 2003.

[10] Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C.: Improvements of image sharing with steganography and authentication, J. Syst. Softw. Vol. 80, No. 7, pp. 1070–1076, 2007.

[11] Fridrich, J., Goljan M., and Rui, D., “Detecting LSB steganography in color and gray-scale images”, IEEE. Multimed. Mag. pp. 22–28, 2001.

[12] Ayidh Alharbi) and M-Tahar Kechadi, "A Steganography Technique for Images Based on Wavelet Transform", International Conference on Future Data and Security Engineering FDSE 2017: Future Data and Security Engineering pp 273-281, 2017.

[13] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee, and Waleed Al-Nuaimy, " Highly Efficient Image Steganography Using Haar Dwt For Hiding Miscellaneous Data", Jordanian Journal of Computers and Information Technology (JJCIT), ISSN: 2413-9351, Vol. 2, No. 1, April 2016.

[14] Xin Wang, "Moving window-based double haar wavelet transform for image processing," in IEEE Transactions on Image Processing, vol. 15, no. 9, pp. 2771-2779, Sept. 2006.

[15] B. Salzberg, "A Modification of Fletcher's Checksum," IEEE Transactions on Communications, vol. 31, no. 2, pp. 295-296, February 1983.

[16] P. Meng, L. Hang, W. Yang, Z. Chen and H. Zheng, "Linguistic Steganography Detection Algorithm Using Statistical Language Model," 2009 International Conference on Information Technology and Computer Science, Kiev, 2009, pp. 540-543.

[17] K. Joshi, R. Yadav and S. Allwadhi, "PSNR and MSE based investigation of LSB," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, 2016, pp. 280-285.

[18] Y. Zhou, M. Yu, H. Ma, H. Shao and G. Jiang, "Weighted-to-Spherically-Uniform SSIM Objective Quality Evaluation for Panoramic Video," 2018 14th IEEE International Conference on Signal Processing (ICSP), Beijing, China, 2018, pp. 54-57.