International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

An Image Steganography Algorithm Using Integer Wavelet Transform and Quadtree Decomposition

Riham O. Elsafy[1], Raafat A. Elkammar[1]

[1]*Department of computer Systems Engineering, Shoubra Faculty of Engineering, Benha University, Cairo, Egypt*

Abstract - *With the increased use of social media and cloud applications our private data exchange over the internet the need to secure these information increases. steganography is one of the historical methodologies used to secure and protect the existence of information. In this paper we present an image steganography technique that uses adaptive quadtree decomposition algorithm with integer wavelet transform to hide secret data, the embedding locations is determined using pseudorandom generator to increase the security of the proposed system. The proposed algorithm provided better results compared to similar algorithms as shown in results.*

Key Words: Steganography, Integer wavelet transform, quadtree decomposition, adaptive segmentation, integer transforms

1.INTRODUCTION

Being able to transform digital media and reproduce them over public networks and also storing data in smart phone and cloud applications which are subjected to intrusion at any time making these data vulnerable. Due to previously mentioned security issue one or more information security methodologies must be use to protect confidential data exchanged namely cryptography and steganography.

Cryptography scrambles data and make it unreadable but also suspicious while steganography conceals the very existence of the data which don't attract any suspicious to the secret data looking plain and regular data to any observer.

Steganography dates back to ancient history where it comes from the Greek words "stegano" which means covered and "graphia" which means writing. In modern world steganography converted from its old techniques to new digital ones that can exploit all most all types of digital files such as text, image, audio, video, etc.

Steganography algorithms have three main conflicting requirements referred to as the magic triangle [1] which is shown in figure 1. They are robustness, undetectability and hiding capacity, whenever an algorithm tries to reach for higher embedding capacity it yields a lower robustness and visual quality. So, the main goal in all steganographic algorithms is to optimize these three requirements.

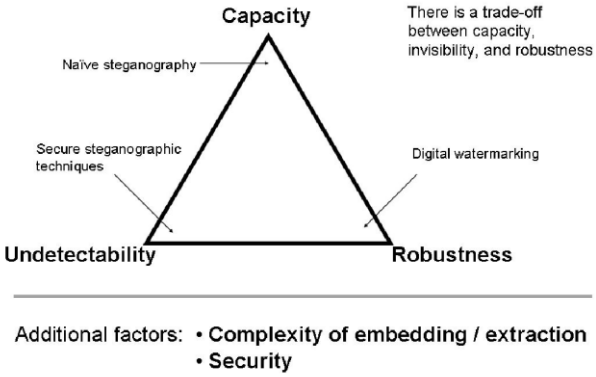


Fig -1: The magic triangle [1]

The most widely used cover media is images due to its redundant information which enables the embedding of large data without being noticeable where the human visual system can hardly detect any distortions in the regions containing complex details in images such as edges and corners.

Image steganography can be classified in many ways [2][3][4] but mostly classified to spatial domain algorithms, transform domain algorithms and model-based algorithms. Spatial domain steganography hides the secret message directly to the pixels of the image [5],[6]. These techniques have the advantage of low computational overhead but they lack robustness and visually detected. Transform domain steganography transforms the image into another transform domain such as Discrete cosine transform, discrete Fourier transform (DFT), discrete wavelet transform (DWT) and other versions of it such as integer wavelet transform (IWT) and dual-tree complex wavelet transform (DTCWT) and many other transforms. The embedding and extracting of secret data in these algorithms are more complex than spatial domain algorithm but they provide more robustness and undetectability. Another important method is the adaptive or model-based steganography it can be used with either spatial domain or which depends on selecting the

regions that adapt to the message content or the nature of the cover to cause minimum distortion [7]. All previous algorithms fall into traditional techniques that can modify an existing cover to some extent. There is another classification emerged in the last few years which is coverless steganography [8] which means that there are no modifications made to cover image and based on the use of generative adversarial networks.

The rest of the paper is organized as follows: related work is presented in section 2. Section 3 presents a brief description of the preliminaries of the integer wavelet transform (IWT) and quadtree decomposition. Section 4 details the proposed system. Evaluation parameters are explained in section 5. Experimental results and comparison with other algorithms are discussed in section 6. Finally, in section 7 discusses conclusion and future work.

2. RELATED WORK

Steganography in transform domain specially in wavelet transform has received much attention. Many researches exploited different types of wavelet transform where in [9] presented a high capacity reversible steganography using multilayer embedding by maximizing the difference between neighboring pixels in a way that is based on the idea of interpolation of images. [10] classify the IWT coefficients based on their first bit of value 1 from the left and don't permit changes to that bit. Integer wavelet transform was combined with multiline directional line encoding (MDLE) that is applied on each 3x3 nonoverlapping coefficient block and the message is inserted into the surrounding eight coefficients and for the LL subband the message is embedded in the edge block after applying edge detection to determine the state of edges of every block [11]. There is a direction to apply other integer transforms such as Catalan transform [12] by converting a group of four pixels using Catalan transform and modifying up to 4 bits of coefficients. Different researches employed chaos mainly to increase the security of the steganographic algorithm due to its sensitivity to initial conditions either by encrypting the secret data as in and or by choosing the bits of the cover to be replaced as in [13], [14] and [15] while in [16] chaotic sequences was used to encrypt the secret message to increase security and the best blocks to hide data are selected using fuzzy inference system (FIS). Adaptive data hiding is based on the idea of selecting the complex and most robust regions in an image for data hiding one way used SURF features [17] also SIFT and ORB characteristics were used [18]. Also, one of the adaptive ways to categorize complex regions in an image is the quadtree decomposition which was used with as in [19]. In [20] and with a combination of DCT, DWT and Laplacian pyramid as in [21].

3. PRELIMINARIES

This section presents a brief explanation of the basic building blocks of the proposed algorithm; integer wavelet transform which is used to transform the image pixels to wavelet coefficients, quadtree decomposition that is used to segment the image into non overlapping blocks of different sizes and finally chaotic mapping which is used to select the embedding locations of the secret message to increase the security of the proposed algorithm. The discussion of these topics will help to have a clear understanding of the proposed algorithm.

3.1 Integer Wavelet Transform

Integer wavelet transform (IWT) is similar to discrete wavelet transform (DWT) where it uses consecutive low pass and high pass filters that divides the image into 4 sub images LL, LH, HL and HH as shown in figure 2. LL sub image represents the approximation of the image while LH, HL and HH represents its details.

(a) (b) (c)

Fig – 2: (a) Lena Original image decomposed using (b) one level IWT (c) two level IWT

The difference between IWT and DWT is that integer wavelet transform maps integer values of image pixels to integer coefficients values which eliminates the precision errors. One way to perform IWT is by using lifting schemes [22] and can be calculated using Eq. (1)

$$D_{1,n} = S_{0,2n+1} - S_{0,2n} \quad ;$$

$$S_{1,n} = S_{0,2n} + \left\lfloor \frac{D_{1,n}}{2} \right\rfloor \quad (1)$$

The inverse integer wavelet transform (IIWT) can be calculated using Eq. (2)

$$S_{0,2n} = S_{1,n} + \left\lfloor \frac{D_{1,n}}{2} \right\rfloor \quad ;$$

$$S_{0,\,2n+1} = D_{0,\,n} + S_{0,\,2n} \quad (2)$$

3.2 Quadtree Decomposition

Quad-Tree image segmentation techniques is an adaptive segmenting scheme that divides a square image into squared non-overlapping blocks with variable size. The size of each block depends complexity and texture of the image. It has different applications such as face recognition, At first, Quadtree divides the image into four equal size blocks then each block homogeneity (the difference between the maximum and minimum pixel value divided by 255) is tested against certain threshold value between 0 and 1[19]. If the homogeneity of a block is greater than the specified threshold then this block is to be further divided into another four blocks. If not, then no further partitioning is made. The sizes of blocks for an image of size m x m have the values of 2^n x 2^n where n=0, 1, 2, 3, 4, 5, 6, …, m/2.

Finally, we will have the cover image divided into n x n adaptive blocks with variable sizes according to the image data. An example of partitioning an image using quadtree is shown in figure 3.

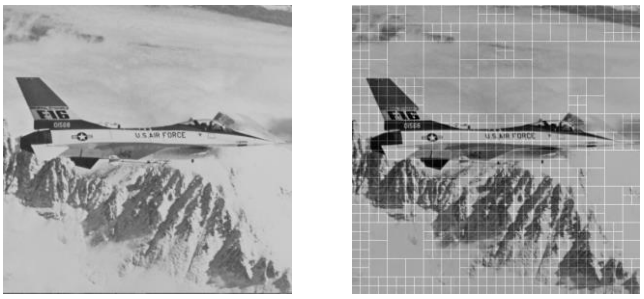


Fig – 3: Illustration of quadtree decomposition on airplane image of size 512 x 512 and variable block sizes

4. PROPOSED ALGORITHM

The proposed algorithm is based on the use of adaptive image segmentation of the quadtree decomposition which is used in many image processing applications along with integer wavelet transform which precision error free transform that ensures the perfect retrieval of the image without precision errors. First the image is segmented into variable size non overlapping blocks using quadtree decomposition then each block is transformed using two level integer wavelet transform (2D-IWT). By setting the number of bits to be replaced in each coefficient (k=1, 2, 3, or 4), the coefficients of the cover image are replaced by the binary stream of the secret message in accordance to the value that each coefficient can hold. Hiding secret information in a sequential order is subjected to detection where it leaves apparent traces of data alteration. In order to avoid that detection, the locations of coefficients to embed data are based on a pseudorandom generator and the seed of the generator acts as the user defined password to increase the security of embedding process. Below is the pseudo code of both embedding and extraction of the secret message.

Algorithm 1: Embedding Algorithm

Input: Cover image C of 512x512, Secret message M, pseudorandom generator seed, decomposition threshold th, Blocks max size bmax, blocks min size bmin

Output: Stego image S

1: BC ← Decompose the cover image (C, th, bmax, bmin)

2: Convert M to binary

3: [LL, LH, HL, HH] ← IWT (BC)

4: Convert each block to binary

5: Generate addressing table using pseudorandom generator

6: set the number of bits to be replaced (k)

7: replace each k bits in CB with message bits

8: stego ← IIWT [LL', LH', HL', HH']

9: return S

Algorithm 2: Extraction Algorithm

Input: stego image S, secret key (initial value of chaotic addressing)

Output: Secret message M

1: BS ← Decompose the stego image (S, th, bmax, bmin)

2: [LL, LH, HL, HH] ← IWT (SC)

3: Convert each block to binary

4: Generate the chaotic addressing table using logistic chaotic map

5: set the number of bits to be extracted (k)

6: Concatenate the bits of each coefficient into the message bits

7: return M

5. EVALUATION METRICS

There are many performance measures according to [23] and [24] that can be used to evaluate a steganographic system performance. The measures we used are Hiding capacity, peak signal to noise ratio (PSNR), Correlation coefficient and structure similarity index measure (SSIM).

5.1 Hiding Capacity

It is the measure of how much secret data is inserted in one pixel. It is measured in bits per pixel (BPP) and it can be calculated according to (1)

$$\text{BPP} = \frac{\textit{Total numbers of embedded bits}}{\textit{Total number of cover image pixels}} \quad (1)$$

5.2 Peak Signal to Noise Ratio (PSNR)

It measures the distortion of the stego-image and it is based on the mean square error between the cover image and the stego-image. It is measured in dB and the image have a good visual quality between 30 and 40 db, values below 30 dB have many distortions and poor visual quality. The PSNR is calculated according to (1)

$$PSNR = 10\, log_{10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

and

$$MSE = \frac{\sum_{i=1}^{N}(C_i - S_i)^2}{N} \quad (3)$$

Where, C_i and S_i are i^{th} pixel value of the original cover and the stego image respectively, and N is the size of the image.

5.3 Correlation Factor (r)

The correlation factor measures the similarity between the cover image and stego image. It is calculated according to (4).

$$r = \frac{\sum_{n=1}^{\infty}(S_i - \mu_S)(C_i - \mu_c)}{\sqrt{\sum_{i=1}^{N}(S_i - \mu_S)^2 \sum_{i=1}^{N}(C_i - \mu_c)^2}} \quad (4)$$

where μ_C and μ_S are the mean pixel values of cover image and stego image respectively.

5.4 Structural Similarity Index Measure (SSIM)

The structural similarity index matrix captures quality of an image as a whole instead of pixel wise metrics which resembles how human visual system works. It is a product of other three measures which are luminance, contrast and structure. it measures the similarity between two images within range -1 means they are completely different and 1 means they are perfectly similar. It is calculated by (5).

$$SSIM = \frac{(2\mu_C\mu_S + C_1)(2\sigma_{CS}^2 + C_2)}{(\mu_C^2 + \mu_S^2 + C_1)(\sigma_C^2 + \sigma_S^2 + C_2)} \quad (5)$$

where,

σ_{CS}^2 is the covariance of cover image C and stego image S while σ_C^2, σ_S^2 are the variance of cover and stego image respectively, C_1 and C_2 are two stabilizing parameters and calculated as follows:

$C_1 = (k_1 L)^2$

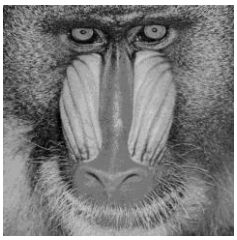
$C_2 = (k_2 L)^2$

L is the dynamic range of pixel values and equals $2^{\#\text{ of bpp}} - 1$ and the constants $k_1 = 0.01$ and $k_2 = 0.03$

6. RESULTS

The proposed system was tested with a data set of cover images shown in figure 4. These cover images are commonly used and tested for performance comparison purposes. All images are of size 512x512.The secret message was a randomly generated binary sequence with the same size as the hiding capacity allowed.

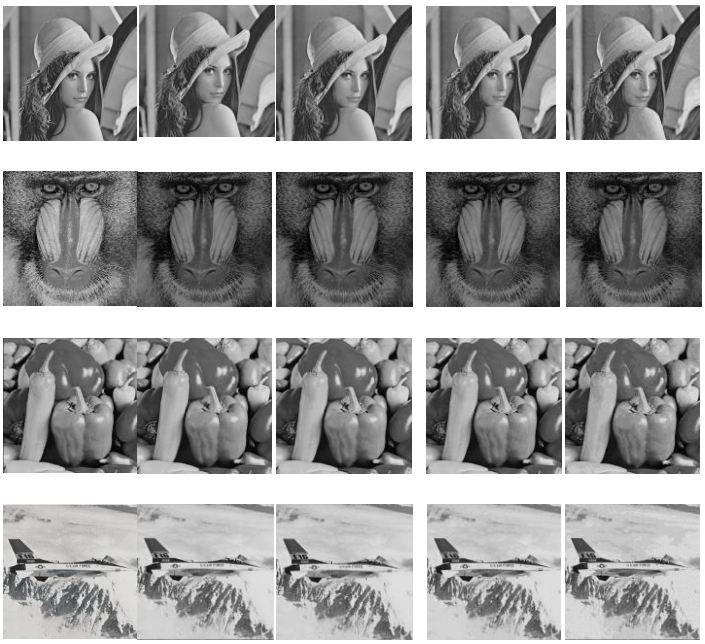
(a) Lena



(b) Baboon


(c) Pepper (d) Airplane

Fig – 4: Cover images



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

Fig – 5: (a) Original cover images and the stego images for (b) 1bpp, (c) 2bpp, (d) 3bpp and (e) 4 bpp hiding capacity

The proposed system hides secret message in 1, 2, 3 or 4 bits per pixel. This allows the hiding of 50% of the cover data. A summary of the values of evaluation metrics discussed in section 5 and estimated for the stego images which are the PSNR, SSIM and correlation for different hiding capacities are given in table 1.

Table – 1: PSNR, SSIM, and correlation for different values of k

K (bits)	Image	PSNR	SSIM	Correlation
1	Lena	47.4647	0.9614	0.9997
	Baboon	47.2739	0.9932	0.9995
	Pepper	47.4171	0.9736	0.9998
	Airplane	47.4966	0.9112	0.9997
2	Lena	41.7195	0.8811	0.9990
	Baboon	41.5665	0.9763	0.9983
	Pepper	41.7052	0.9133	0.9992
	Airplane	41.7582	0.7976	0.9990
3	Lena	35.8093	0.7241	0.9963
	Baboon	35.7182	0.9252	0.9934
	Pepper	35.8277	0.7695	0.9971
	Airplane	35.7421	0.6432	0.9960
4	Lena	29.4963	0.5314	0.9845
	Baboon	29.7171	0.8071	0.9743
	Pepper	29.5415	0.5565	0.9878
	Airplane	29.3624	0.4819	0.9829

The resultant stego images of along with the original cover image for hiding I, 2, 3 and 4 bits per pixel (bpp) of the secret message. are shown in figure 5 while the histograms of the four cover images and stego images for each of different value of hiding capacity is shown in figure 6 to figure 9. When hiding only one bit in each pixel (12% of the cover image data) the histogram shows no change and the values start to get smoother when increasing number of bits being modified in the integer wavelet coefficients of the cover with the secret message bits until we reach hiding 50% of the cover data, we get PSNR value of 29.5 dB on average which falls below the acceptable range (30 db).

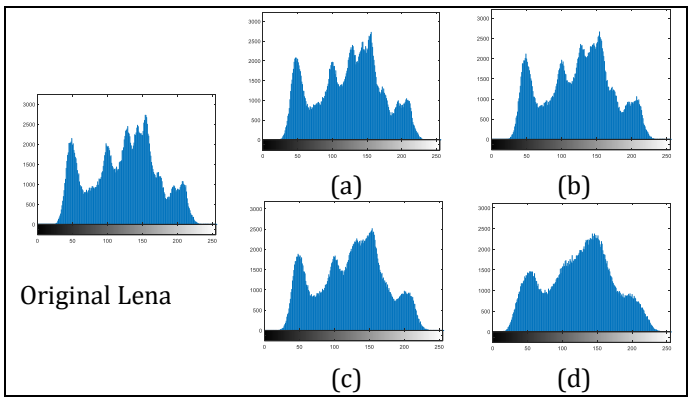


Fig -6: The histograms of original cover image Lena and stego images at different hiding capacities (a) 1bpp, (b) 2bpp, (c) 3bpp and (d) 4bpp

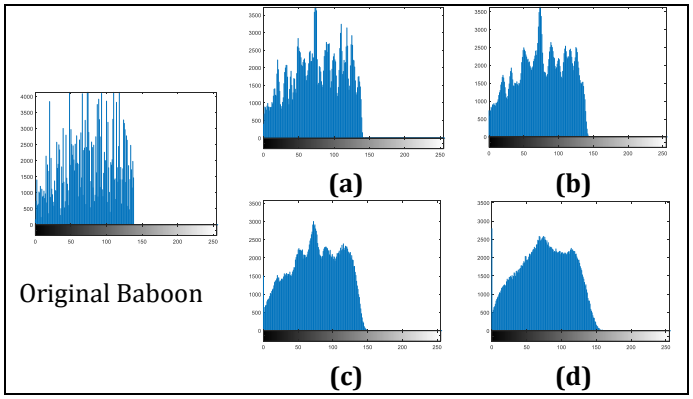


Fig -7: The histograms of original cover image Baboon and stego images at different hiding capacities (a) 1bpp, (b) 2bpp, (c) 3bpp and (d) 4bpp

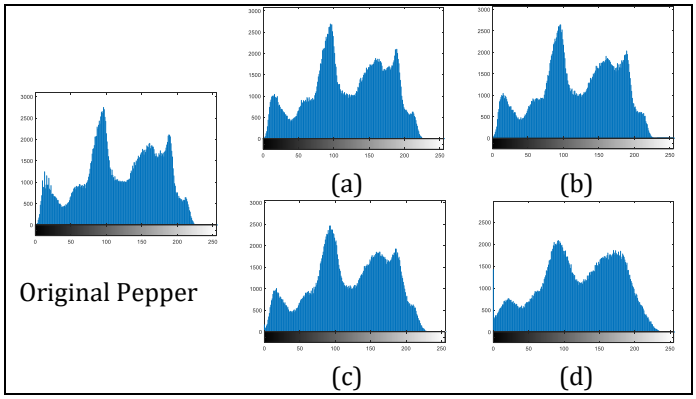


Fig -8: The histograms of original cover image Peppers and stego images at different hiding capacities (a) 1bpp, (b) 2bpp, (c) 3bpp and (d) 4bpp

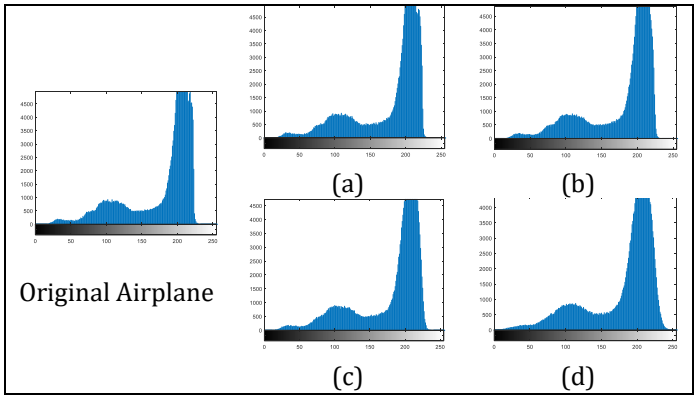


Fig -9: The histograms of original cover image Airplane and stego images at different hiding capacities (a) 1bpp, (b) 2bpp, (c) 3bpp and (d) 4bpp

The proposed system was tested against some state-of-the-art algorithms, Zahng [11], Mukhopadhyay [12] and Nazari [16]. The comparison was based on the same cover images Lena, Baboon, Peppers and airplane with the same size 512x512. The values of obtained hiding capacities and the corresponding PSNR values are shown in table 2. The values shows that the proposed system outperforms all algorithms except when hiding only one bit per pixel in [12] which uses Catalan transform.

Table – 2: Comparative results of proposed algorithm

Algorithm		Lena	Baboon	Peppers	Airplane
	HC	PSNR			
Zahng [11]	1.9	41.7	41.04	41.15	41.18
Mukhopadhyay [12]	1	**48.62**	**48.62**	**48.62**	**48.64**
	2	40.93	40.92	40.91	40.92
	3	34.23	34.24	34.23	34.24
	4	27.93	27.93	27.95	27.93
Nazari [16]	0.35	49.648	41.647	45.518	53.448
Proposed algorithm	1	47.464	47.273	47.417	47.496
	2	**41.719**	**41.566**	**41.705**	**41.758**
	3	**35.809**	**35.718**	**35.827**	**35.742**
	4	**29.496**	**29.717**	**29.541**	**29.362**

7. CONCLUSION AND FUTURE WORK

Integer wavelets shows precision error free and faster computations as compared to other transforms. Quadtree decomposition provides an adaptive way to divide the cover image into blocks according to their complexity. The proposed algorith3m showed better results than other algorithms as shown in table 2 for hiding 1, 2, and 3 bpp producing PSNR value above 30 dB while fails to achieve higher PSNR values at hiding 4 bpp (PSNR averages to 29 dB).

As a future direction the proposed algorithm can be modified to increase hiding capacity and its security, also the use of other transforms such as quadtree complex wavelet or other integer transform in order to increase the visual quality. Also investigating the application of the proposed algorithm on colored images with different color spaces can add different perspective to the visual quality against hiding capacity. Another direction of improvement could be the use of evolutionary algorithms such as particle swarm optimization.

REFERENCES

[1] J. Fridrich, "Applications of data hiding in digital images," in ISSPA '99. Proceedings of the Fifth International Symposium on Signal Processing and its Applications (IEEE Cat. No.99EX359), vol. 1, p. 9, doi: 10.1109/ISSPA.1999.818099.

[2] S. Jeevitha and N. Amutha Prabha, "A comprehensive review on steganographic techniques and implementation," ARPN J. Eng. Appl. Sci., vol. 13, no. 17, pp. 4780–4791, 2018.

[3] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, no. xxxx, pp. 299–326, 2019, doi: 10.1016/j.neucom.2018.06.075.

[4] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Comput. Sci. Rev., vol. 13–14, no. C, pp. 95–113, 2014, doi: 10.1016/j.cosrev.2014.09.001.

[5] L. Yu, Y. Zhao, R. Ni, E. Member, and T. Li, "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm," vol. 2010, 2010, doi: 10.1155/2010/876946.

[6] S. Rahman et al., "A novel approach of image steganography for secure communication based on LSB substitution technique," Comput. Mater. Contin., vol. 64, no. 1, pp. 31–61, 2020, doi: 10.32604/CMC.2020.09186.

[7] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," IEEE Access, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[8] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," IEEE Access, vol. 7, pp. 171372–171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[9] M. Tang, J. Hu, and W. Song, "A high capacity image steganography using multi-layer embedding," Optik (Stuttg)., vol. 125, no. 15, pp. 3972–3976, 2014, doi: 10.1016/j.ijleo.2014.01.149.

[10] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform," Multimed. Tools Appl., vol. 77, no. 11, pp. 13133–13144, 2018, doi: 10.1007/s11042-017-4935-z.

[11] H. Zhang and L. Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," Signal Process. Image Commun., vol. 78, no. July, pp. 331–344, 2019, doi: 10.1016/j.image.2019.07.019.

[12] S. Mukhopadhyay, S. Hossain, S. K. Ghosal, and R. Sarkar, "Secured image steganography based on Catalan transform," Multimed. Tools Appl., pp. 14495–14520, 2021, doi: 10.1007/s11042-020-10424-4.

[13] O. N. Kadhim and Z. M. Hussain, "Information hiding using chaotic-address steganography," J. Comput. Sci., vol. 14, no. 9, pp. 1247–1266, 2018, doi: 10.3844/jcssp.2018.1247.1266.

[14] J. Sharafi, Y. Khedmati, and M. M. Shabani, "Image steganography based on a new hybrid chaos map and discrete transforms," Optik (Stuttg)., vol. 226, p. 165492, 2021, doi: 10.1016/j.ijleo.2020.165492.

[15] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map," Multimed. Tools Appl., vol. 76, no. 11, pp. 13493–13510, 2017, doi: 10.1007/s11042-016-3722-6.

[16] M. Nazari and I. Dorostkar Ahmadi, "A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity," Multimed. Tools Appl., vol. 79, no. 19–20, pp. 13693–13724, 2020, doi: 10.1007/s11042-019-08415-1.

[17] N. Hamid, A. Yahya, R. B. Ahmad, and O. Al-Qershi, "Characteristic region based image steganography using Speeded-Up Robust Features technique," 2012 Int. Conf. Futur. Commun. Networks, ICFCN 2012, pp. 141–146, 2012, doi: 10.1109/ICFCN.2012.6206858.

[18] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-qershi, "A Comparison between Using SIFT and SURF for Characteristic Region Based Image Steganography," Int. J. Comput. Sci. Issues, vol. 9, no. 3, pp. 110–116, 2012.

[19] J. Kumar, "A novel approach to image steganography using quadtree partition," Proc. 2016 2nd Int. Conf. Next Gener. Comput. Technol. NGCT 2016, no. October, pp. 93–98, 2017, doi: 10.1109/NGCT.2016.7877396.

[20] T. Rabie and I. Kamel, "Toward optimal embedding capacity for transform domain steganography: a quad-tree adaptive-region approach," Multimed. Tools Appl., vol. 76, no. 6, pp. 8627–8650, 2017, doi: 10.1007/s11042-016-3501-4.

[21] T. Rabie, M. Baziyad, and I. Kamel, "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid," Multimed. Tools Appl., vol. 77, no. 18, pp. 23673–23698, 2018, doi: 10.1007/s11042-018-5713-2.

[22] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. L. Yeo, "Wavelet Transforms That Map Integers to Integers," Appl. Comput. Harmon. Anal., vol. 5, no. 3, pp. 332–369, 1998, doi: 10.1006/acha.1997.0238.

[23] A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques," Int. Conf. Res. Adv. Integr. Navig. Syst. RAINS 2016, 2016, doi: 10.1109/RAINS.2016.7764399.

[24] D. Laishram and T. Tuithung, "3 rd International Conference on Internet of Things and Connected Technologies A Survey on Digital Image Steganography : Current Trends and Challenges."