EFFICIENT STEGANOGRAPHY SCHEME FOR COLOR IMAGES BASED ON WAVELETS AND CHAOTIC MAPS

Hikmat N. Abdullah [1], Sura F. Yousif [2], Alejandro A. Valenzuela [3]
[1] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
[2] College of Engineering, Diyala University, Baghdad, Iraq
[3] EMT Department, Bonn-Rein-Sieg University, Germany
hikmat.abdullah@coie-nahrain.edu.iq [1], sura.fahmy@yahoo.com [2], alejandro.valenzuela@h-brs.de [3]
Received:4/11/2019, Accepted:15/12/2019

***Abstract*- In this paper, a combination of spatial domain as well as transformation domain with the aid of chaotic sequences is used to propose an efficient steganography scheme for color images. The transform domain uses Discrete Wavelet Transform (DWT) for embedding the cover and secret images. Chaotic sequences are used for two purposes: first, to scramble the secret color image before hiding. Second, to randomly select the locations of the cover image for embedding. The two images are then merged together into a single image and the stego image is formed by applying IDWT. The secret image is extracted from the stego image without the need to the original cover image. The simulation results are evaluated in terms of Mean Square Error (MSE), correlation, and Peak Signal to Noise Ratio (PSNR) demonstrate that the proposed scheme has better robustness than the previous schemes in the literature in the presence of common image attacks including filtering and noise attacks. The obtained results for maximum PSNR and correlation were 76.8 dB and 99.99% for the stego image while for the extracted secret image were 55.4 dB and 100%.**

keywords: **Chaotic sequences, Steganography, Discrete wavelet transform, Color image secuity.**

I. INTRODUCTION

With the rapid growth of internet networks and technologies, the demand for information security is highly increased. To guarantee the security of sent information, one of the most important techniques that has been developed is steganography. Steganography deals with covert communication. First, important information such as graphics or sound is hidden in host data, called carriers or covers. These may be texts, audio files, videos or digital images. Then, they are transmitted to the receiver secretly [1]. Steganography can be characterized by three aspects that are connected to each other: security, capacity, and robustness. Security refers to an attacker's inability to detect the embedded information [2]. Capacity refers to the amount of embedded information in the cover object. Robustness is a measure of how much difficulty is associated with removal of embedded information in the presence of attacks. Steganography can further be categorized by two important types of how the cover object hides the information: spatial domain and transform or frequency domain. Spatial domain steganography hides the secret data in the least significant bits of the host image pixels which are selected randomly or sequentially. This method allows simple hiding and high embedding capacity but has low resistance against attacks such as lossy compression or filtering [3]. Transform domain steganography hides the secret data basically in the transform coefficients of the host image. It satisfies the criteria of robustness and of transparency. There are many transform domain variations that have been proposed such as Integer Wavelet Transformation (IWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [4]. DWT has been used lately in many mathematical and practical applications such as steganography due to the many advantages it offers. The hierarchical representation of DWT allows the multiresolution detection of the embedded information. Such approaches basically address the robustness and

capacity of the steganography characteristics [5]. DWT is used in this scheme as a transform domain. Chaotic sequences are random sequences recently utilized to increase the security of steganography schemes. In 1963, Edward Lorenz proposed the first chaotic system. Many different research areas established since then in engineering and other fields of sciences. The most significant features of chaos is the sensitivity to parameters changes the initial conditions. In steganography applications, chaotic maps are used to select the embedding positions of the cover image and the bit positions that are used for manipulation. Chaotic signal looks like noise but they are completely deterministic. This means the signal value can be reproduced if the primary values and the map function are found [6].

II. Related Work

D. Bandyopadhyay et al. presented a steganography scheme to embed a secret message within the color image according to the chaotic map [7]. The secret color image is encrypted using a logistic map to raise the security before the embeddeding in the LSB of the cover image. G. Prabakaran et al. proposed color image steganography based on DWT, IWT and Arnold transforms [8]. Arnold transform is used to scramble the secret message, then both cover image and secret message are decomposed using DWT and IWT. Alpha blending is used to mix the secret message with the cover image. In [1], A. Sharif et al. introduced a steganography technique to embed a secret message within the color image based on spatial domain and three dimensional chaotic maps. Chaotic maps are used for identifying the rows and columns numbers as well as the color components of pixels, accordingly. They also used for selecting desirable hosted pairs or triples pixel positions for embedding least and most significant bits of the secret message. In [2], M. J. Bawaneh et al. presented a gray scale image steganography technique based on LSB embedding and image segmentation. In this technique, different types of images are transformed into a virtual gray scale of 24 bits and the possible segments within the image are found. Then the possible areas for each segment and corresponding boundaries are computed. N. Kaushik et al. suggest a steganographic system that depends on chaos theory and DWT [3]. A Chaotic sequence is used to encrypt the secret image by applying spatial domain (LSB) and then frequency domain stegnography (DWT) before embedding the information into the color cover image. In [5], Reshma et al. proposed a secure image steganography by combining chaotic maps and watermarking techniques. To increase the security, a logistic map is used to generate the chaotic map. In all previous works mentioned above, either spatial domain or transform domain is used to achieve steganography. In the paper, an efficient steganography scheme based on the combination of both spatial domain and transform domain (DWT) is proposed. This approach is used to improve the image steganography in terms of embedding capacity without any noticeable distortion to the cover image, image quality and robustness against image manipulation attacks. The secret image in the proposed scheme is retrieved without requiring the original cover image.

III. Chaotic Maps

Recently, chaotic maps are in digital steganography applications to increase the security. In secure communications, chaotic maps have many compelling features such as high sensitivity to the primary conditions, the outspreading of orbits over the entire space, sensitivity to control parameters, ergodicity, and random behavior. These excellent properties make

chaotic maps very good candidates for data hiding applications. Chaotic maps such as the logistic map, Tent map and Henon map have been used widely to generate random sequences [5], [9].

A. Logistic Map

In 1976, Robert May was the first to ingratiate the logistic map for estimations of population growth rates. It is one of the simplest nonlinear maps, but with complex dynamics. Through dynamical nonlinear equations, this map uses polynomial iterations that diverge iteratively to a chaos behavior. It can be defined as:

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

where x_n is the nth value of the chaotic map given that the initial value should be within the range (0, 1) and r a factor that controls the map behavior. To introduce the chaotic activity, the value of this factor should be between 3.57 and 4 [10].

B. Tent Map

It is a one dimensional piecewise linear chaotic map with simple calculations compared to logistic map. This chaotic map maps the point xn into another point according to the difference equations below:

$$\begin{aligned} x_{n+1} &= rxn \qquad for\, 0 \leq x_n < 0.5 \\ x_{n+1} &= r(1 - x_n) \quad for\, 0.5 \leq x_n \leq 1 \end{aligned} \tag{2}$$

where r represents a positive real number bounded in the range [0,2]. Wide range of dynamical behavior has been demonstrated with tent maps based on different values of r [11].

C. Henon Map

The Henon map or Henon model is an interesting map because it consists of two variables: x and y. This map is represented the following difference equations

$$\begin{aligned} x_{n+1} &= 1 - ax_n^2 \\ y_{n+1} &= bx_n \end{aligned} \tag{3}$$

with a and b representing control parameters. The chaotic and periodic attractors can be found depending on choice of a and b. A wide spectrum of nonlinear behavior is obtained by Hennon map e.g. a strange attractor. To generate iterations of chaotic sequences, a and b should have the values 1.4 and 0.3 respectively [12].

IV. The Proposed Algorithem

A digital image steganography technique that combines both spatial and transform domains is proposed. It uses chaotic maps which are highly sensitive to the initial conditions to increase the security of the embedding and extraction schemes. The combination of chaos with the DWT domain will increase the robustness of this algorithm. The proposed algorithm hides a color secret image of variable sizes into a color cover image of the size 512×512. It has two complementary parts: the embedding process at the sender side and the extraction process at the recipient side.

A. Embedding Process

The embedding process for the proposed algorithm is shown in Fig. 1. It includes steps followed to perform the proposed steganography scheme. First of all, since the secret and cover images are color images, they are separated to three channels: red, green and blue at the sender side. Next, a two level DWT is performed in each channel of the cover image. Three types of chaotic maps are then generated: a logistic map, a tent map and a Henon map. Each channel of the secret image is scrambled using a Henon map. After that, a one level DWT is performed to each scrambled channel of the secret image. The embedding process is performed using logistic and tent map. Logistic map will choose randomly the proper coefficients for the embedding process in the cover image, while the tent map will choose the proper bits in the chosen coefficients and substitute them with the coefficients of the secret image. If we take for example the red channel, each coefficient in the cover and final secret images consists of 8 bits, if the value of pseudorandom number generated by the logistic map equals to one, then the coefficient number one is used to embed the first two bits of the resulting secret image. If the value of pseudorandom number generated by the logistic map equals to two, then the coefficient number two is utilized to embed the second two bits of the final secret image and so on. The embedding process is performed by replacing the first two bits of the final secret image by the first two bits of the first coefficient of the cover image and the second two bits of the final secret image by the first two bits of the second coefficient of the cover image. The choice of which two bits are selected from the eight bits in each coefficient of the cover image to embed the secret coefficients depends on the tent map. If the value of the pseudorandom number generated by the tent map equals to two, then the two LSB are used from each coefficient of the cover image for the embedding process. This operation is continued until overall bits of the final secret image are totally embedded in the coefficients of the cover image. Each layer of the secret image is embedded in the corresponding layer of the cover image. A two level IDWT is then performed to each channel of the cover image: red, green and blue after the embedding process has been completed successfully. Finally, the three channels are concatenated in order to get the stego image. The preparation of both secret and cover images is shown in Fig. 2 and Fig. 3 respectively. The stego image is very similar to the cover image as shown in Fig. 4.

B. Extraction Process

The extraction process for the proposed algorithm is shown in Fig. 5. It is similar to the embedding process at the sender side but with reverse operations. After receiving the stego image from the source, it is separated to three channels: green, red and blue. Next, a two level DWT is performed to each channel. The recipient should have the same three keys that are used in the embedding process at the sender: the logistic map, the tent map and Henon map in order to reconstruct or recover the secret image. After that, a one level IDWT is performed to each recovered channel of the scrambled secret image. The resulting scrambled image is then descrambled using a Henon map. Finally, the three channels are concatenated to get the original secret image.

V. Experimental Results

The performance of the proposed algorithm was evaluated by three benchmark techniques. Firstly, by the Mean Square Error (MSE) which demonstrate the difference between stego and cover the images. Secondly by the Peak Signal to Noise

Ratio (PSNR) which is a measure of amount of distortion in the stego image after embedding the secret information in the cover. Finally, by the correlation or similarity measure which is used to compute the similarity between the stego and cover images. Both images are highly correlated when the value of the computed correlation coefficient is close to one [1, 13]. The proposed algorithm is tested and implemented using MATLAB R2017a as simulation tool on a personal computer with an Intel Core i3 processor running at a clock rate of 2.40 GHz. To demonstrate the performance of the proposed algorithm, three color test images are used as cover images which are: Couple, Tiffany and Peppers. These images are found in many digital image processing, compression and steganography works. The size of these images is considered 512×512. The color secret image is Sailboat of different sizes. The secret and cover images are shown in Fig. 6. The simulation results are summarized in Tables I and II for the stego and extracted secret images. According to Table I the MSE will increase with capacity or payload while the PSNR and correlation will decrease and vice- versa. This means that a trade- off between capacity, PSNR and correlation has to be made to satisfy these requirements. For the stego images in Table I, minimum MSE, maximum PSNR and correlation values of 0.0014, 76.8236dB and 0.9999 respectively occurred when the cover image is Couple and the secret image (Sailboat) of size (32×32). These values become 0.0252, 64.1217dB and 0.9998 for MSE, PSNR and correlation when the secret image increases to a size of 256×512 for the same cover image, maintaining high imperceptibility and a good image quality. The extracted secret image in Table II can be correctly extracted from the stego image under no attack because the correlation between the secret image at the sender and the extracted secret image at the recipient is one, this means that these two images are same.

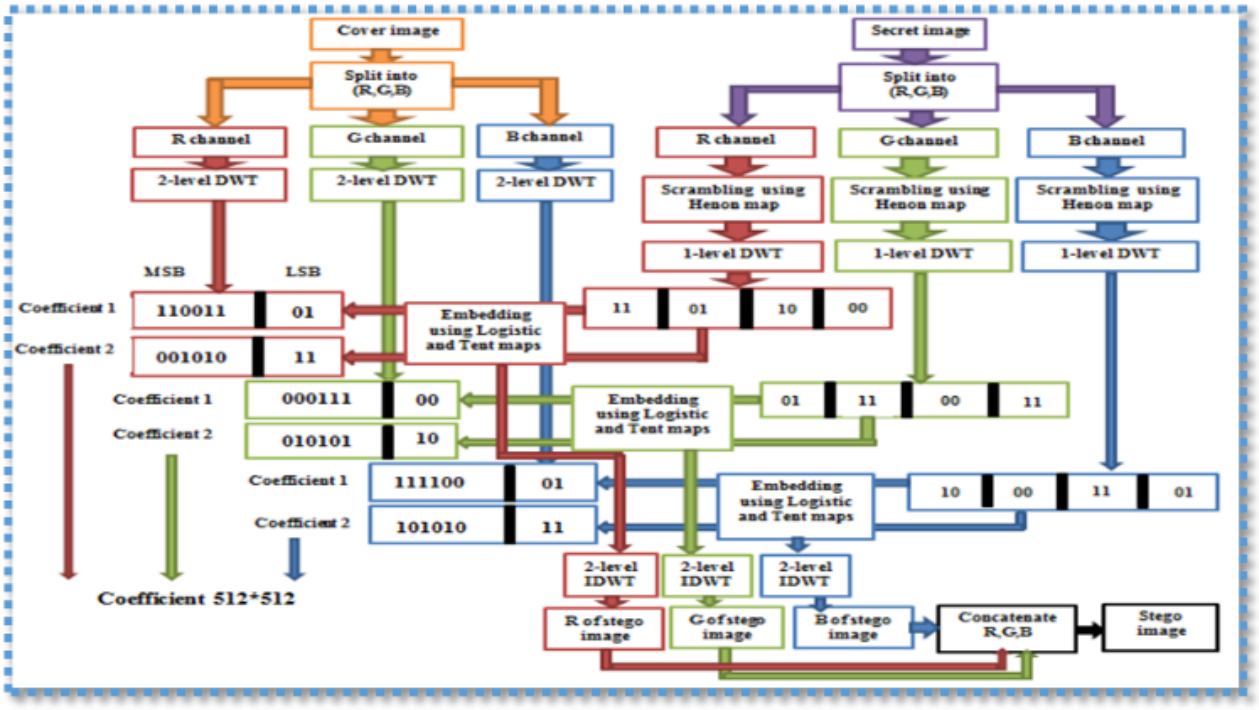

Figure 1: Block diagram of the embedding process

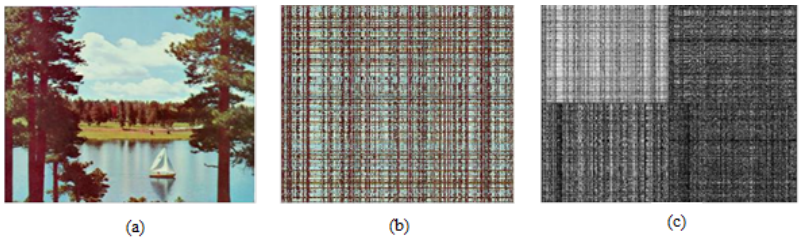

Figure 2: (a) Secret image, (b) Scrambled image, (c) One level DWT of the scrambled image

Figure 3: (a) Cover image, (b) Two level DWT of the cover image

Figure 4: (a) Cover image, (b) Stego image.

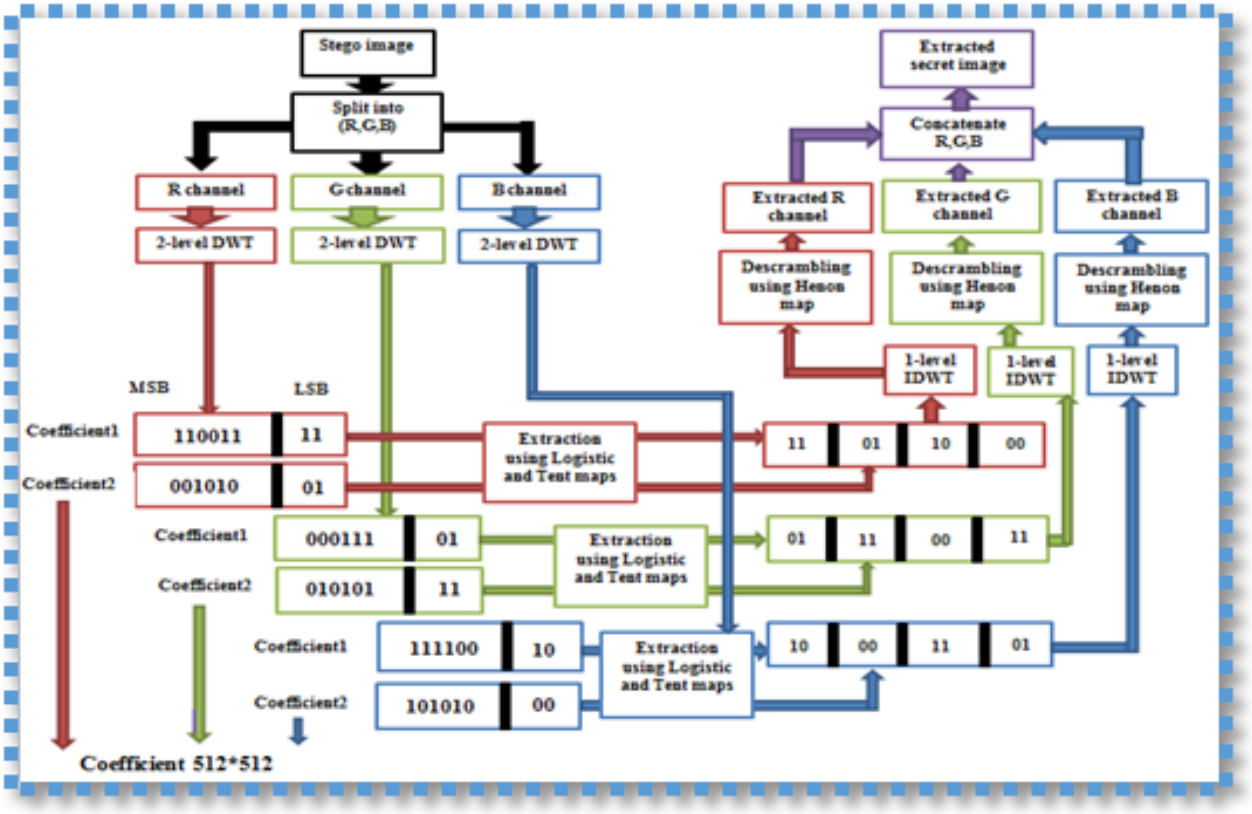

Figure 5: Block diagram of the extraction process

TABLE I
MSE, PSNR AND CORRELATION VALUES OF THE STEGO IMAGE

Dimension of the secret image	Stego image	MSE	PSNR (dB)	Correlation
$32 * 32$	Couple	0.0014	76.8236	0.9999
$32 * 64$		0.0019	75.3414	0.9999
$64 * 64$		0.0030	73.3135	0.9999
$64 * 128$		0.0041	71.9807	0.9999
$128 * 128$		0.0063	70.1372	0.9999
$128 * 256$		0.0113	67.6089	0.9998
$256 * 256$		0.0168	65.8889	0.9998
$256 * 512$		0.0252	64.1217	0.9998
$32 * 32$	Tiffany	0.0051	71.0258	0.9999
$32 * 64$		0.0072	69.5501	0.9998
$64 * 64$		0.0116	67.4729	0.9998
$64 * 128$		0.0158	66.1482	0.9998
$128 * 128$		0.0241	64.3077	0.9998
$128 * 256$		0.0431	61.7893	0.9998
$256 * 256$		0.0643	60.0508	0.9998
$256 * 512$		0.0950	58.3516	0.9997
$32 * 32$	Peppers	0.0052	70.9885	0.9999
$32 * 64$		0.0072	69.5406	0.9998
$64 * 64$		0.0117	67.4546	0.9998
$64 * 128$		0.0154	66.2556	0.9998
$128 * 128$		0.0236	64.3963	0.9998
$128 * 256$		0.0419	61.9035	0.9998
$256 * 256$		0.0633	60.1167	0.9998
$256 * 512$		0.0925	58.4699	0.9997

Figure 6: Cover images (a) Couple, (b) Tiffany, (c) Peppers, (d) Secret image (Sailboat)

TABLE II
MSE, PSNR AND CORRELATION VALUES OF THE EXTRACTED SECRET IMAGE

Dimension of the secret image	Extracted secret image (Sailboat)		
	MSE	PSNR (dB	Correlation
$32 * 32$	0.1891	55.3633	1
$32 * 64$	0.1831	55.5038	1
$64 * 64$	0.1863	55.4292	1
$64 * 128$	0.1807	55.5621	1
$128 * 128$	0.1888	55.3698	1
$128 * 256$	0.1850	55.4584	1
$256 * 256$	0.1888	55.3713	1
$256 * 512$	0.1741	55.7231	1

VI. ROBUSTNESS OF THE PROPOSED ALGORITHM

In order to measure the resistance of the proposed algorithm, several image processing attacks including filtering and noise attacks are applied to the stego image. They include the cover image Peppers when the secret image is of size 256×256. The resistance analysis results of these attacks are listed in Table III for the stego and extracted secret images. As shown in this table, although of the presence of different types of attacks, the obtained PSNR and correlation values for the stego image are satisfactory especially for salt and pepper noise, Gaussian noise and blurring noise attacks. Even for other types of attacks the obtained values are acceptable (more than 30dB and around unity correlation). This proves the good robustness for the proposed algorithm. Further, PSNR of the extracted image is about 13.3 dB and the correlation is about 0.78 regardless of the attack type which is considered superior as compared to existing methods.

TABLE III
SIMULATION RESULTS OF PSNR AND CORRELATION UNDER DIFFERENT ATTACKS

Type of attack	Stego image (Peppers)		Extracted secret image (Sailboat)	
	PSNR (dB)	Correlation	PSNR (dB)	Correlation
Salt and pepper noise (density =0.0001)	53.3308	0.9985	13.3063	0.7862
Poisson noise	32.3995	0.9956	13.2865	0.7846
Speckle noise (density =0.01)	30.3300	0.9929	13.3031	0.7860
Gaussian noise (G=0, h=0.000001)	61.0818	0.9998	13.2915	0.7854
Blurring (radius=0.5)	76.2884	0.9999	13.3303	0.7781
Sharpening $(3 * 3)$	24.5804	0.9760	13.2646	0.7761
Median filter $(3 * 3)$	36.2374	0.9982	13.3274	0.7841
Low pass filter $(3 * 3)$	30.4838	0.9932	13.2632	0.7861
Wiener filter $(3 * 3)$	35.6246	0.9979	13.2784	0.7864
Gaussian low pass filter $(3 * 3)$	32.0563	0.9953	13.3154	0.7838

VII. COMPARISION WITH OTHER APPROACHES

A. Without Attack

The proposed algorithm is also compared with other similar existing approaches in [7], [8] in terms of PSNR for the no attack case. In this comparison, the cover image Peppers and the secret image (Sailboat) of size 256×256 from Table I are considered and the results are given in Table IV. It is clear that the algorithm outperforms the previous approaches in terms of PSNR, which means that it produces lower visual distortion to the cover image after embedding the secret image. The gain obtained in PSNR when compared with [8], which has the highest PSNR, is 0.2067dB.

B. With Attack

Table V compares the proposed algorithm to the previous approach in [8] in terms of PSNR for the attacking case. The cover image Peppers and the secret image (Sailboat) of the same size in the previous comparison are considered in this comparison. It can be seen from Table V that the proposed algorithm is more robust against several image processing attacks than the existing approach for every attack in terms of PSNR. As compared with [8], the obtained gain in PSNR using the proposed algorithm for salt and pepper noise attack is 4.9836dB. The gain obtained in PSNR for Gaussian noise attack is 9.8107dB. The gain obtained in PSNR for blurring attack is 14.7053dB. The two comparisons in Tables IV and V with and without attack concludes the superiority of the proposed algorithm.

TABLE IV
COMPARISON OF PROPOSED ALGORITHM WITH PREVIOUS APPROACHES WITHOUT ATTACK

Algorithm	Ref.[7]	Ref.[8]	Proposed algorithm
PSNR (dB)	58.94	59.91	60.1167

TABLE V
COMPARISON OF PROPOSED ALGORITHM WITH SIMILAR PREVIOUS APPROACHES WITH ATTACK

Type of attack	PSNR (dB)	
	Ref.\cite{G}	Proposed algorithm
Salt and pepper noise (density =0.0001)	48.3472	53.3308
Gaussian noise (G=0, h=0.000001)	51.2711	61.0818
Blurring (radius=0.5)	61.5831	76.2884

VIII. CONCLUSIONS

Steganography is not always the best solution, neither for secrecy nor for encryption. But if we combine these two techniques, then we will have two layers of protection. In this scheme, the secret message is scrambled or encrypted using

chaotic maps to enhance the security of the proposed algorithm, then it is hidden in the LSB of the cover image after transforming both the cover and the secret images into the wavelet domain. The wavelet domain allows perfect embedding and reconstruction of the secret message. The stego image can be transmitted to the destination without revealing that secret data is being exchanged. Furthermore, if an attacker tries to defeat the proposed algorithm by detecting the hidden message from the stego image, he will still need the three keys (logistic map, tent map and Henon map) to decrypt the message. The ability of wavelet transform to introduce sparsity and compressing data will lead to increase the capacity or payload of the steganography process which reaches up to $3/4$ of the size of the cover image when the secret image is of size 256x512 in the proposed algorithm with very little effect on the statistical nature of the stego image. The proposed algorithm attempts to overcome the demerits of previous image steganography approaches. The drawn results from the simulations in terms of MSE, PSNR and correlation show high levels of security, good visual quality of the stego image and perceptual invisibility of the secret image, as well as strong robustness in the operation of noise and filtering attacks. Performance analysis of the algorithm in comparison with previous approaches conclude that the scheme is superior in terms of PSNR for the stego image with and without attacks.

REFERENCES

[1] A. Ansari, M. Mohammadi, and M Parvez, " A Comparative study of Recent Steganography Techniques for Multiple Image Formats" , International Journal of Computer Network and Information Security, Vol. 11, No. 1, January 2019, pp. 11- 25.
[2] M. J. Bawaneh and A. A. Obeidat, " A Secure Robust Gray Scale Image Steganography Using Image Segmentation" , Journal of Information Security, Vol. 7, No. 1, 2016, pp. 152- 164.
[3] M. Hussain et. al. , " Image steganography in spatial domain: A survey" , Journal of Image Communication, ScienceDirect, Elsevier, Vol. 65, July 2018, pp. 46- 66.
[4] R. J. S. Kahlon and V. Bhardwaj, " A Secure Image Steganography Using Bit Shift Encryption & MLSB Approach" , International Journal of Science and Research (IJSR), Vol. 5, Issue. 7, July 2016, pp. 408- 412.
[5] Hikmat N. Abdullah, Sura F. Yousif and Alejandro A. Valenzuela, " Wavelet Based Image Steganographic System using Chaotic Signals" , Proceedings of 6th IEEE International Conference on Information Communication and Management ICICM 2016, 29- 31 October 2016, London, United Kingdom, pp. 130- 135.
[6] L. P. Gagnani and S. Varjani, " Survey of 3D Chaotic Map Techniques for Image Encryption" , International Journal of Science and Research (IJSR), Vol. 4 Issue. 12, December 2015, pp. 1000- 1004.
[7] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta, " A novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain " , International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 3, No. 1, February 2014, pp. 11- 22.
[8] G. Prabakaran, R. Bhavani, and M. Kiruthika," A Novel Secure Color Image Steganography Based on Denoising Methods in DWT and IWT Techniques" , International Conference on Engineering Trends and Science & Humanities (ICETSH), December 2015, pp. 50- 55.
[9] A. Kumar, A. Rajpoot, K. K. Shukla, and S. Karthikeyan , " A Robust Method for Image Steganography based on Chaos Theory" , International Journal of Computer Applications, Vol. 113 - No. 4, March 2015, pp. 35- 41.
[10] N. C. Patil and V. V. Patil, " Advance Data Hiding in Spatial Domain Image Using Chaotic Map" , International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 5, Issue 1, January 2016, pp. 59- 63.
[11] P. Kori, R. Dubey, and V. Richhariya, " Survey on Double Phase Image Encryption and Decryption using Tent Map and Chaotic Logistic Map" , International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 4, Issue 11, November 2015, pp. 3694- 3700.
[12] M. F. M. Mursi and A. H. Abd El-aziem, " Applications of Chaotic Maps and Coding for Secure Transmission of Images over Wireless Channels" , Wseas Transactions on Computer Research, Vol. 4, 2016, pp. 86- 95.
[13] H. Song et. al. , " Security Measure for Image Steganography Based on High Dimensional KL Divergence" , Journal of Security and Communication Networks, Hindawi, Vol. 2019, Article ID 3546367, pp. 1- 13, April 2019.