Wireless Personal Communications (2020) 110:321–337
https://doi.org/10.1007/s11277-019-06730-2

An Efficient Image Steganography Approach over Wireless Communication System

Asmaa Abdelmonem Eyssa[1] · **Fathi Elsaid Abdelsamie**[2] · **Abdelaziz Elsaid Abdelnaiem**[1]

Published online: 21 September 2019

Abstract
This paper presents a robust color image steganography approach for image communication over wireless communication systems. The objective of this approach is to hide three color images in one color cover image to increase the capacity of hiding as most previously published steganography approaches suffer from a capacity problem. Moreover, the investigation of wireless communication of steganography images is presented in this paper to study the sensitivity of extraction of hidden images to the channel degradation effects, which is not studied appropriately in the literature. The proposed approach depends on the Discrete Cosine and Discrete Wavelet transform. The cover image is first transformed to luminance and chrominance components for embedding the images to be hidden. The secret images are encrypted by chaotic Baker map, which is a good representative of the family of permutation-based algorithms, which tolerate the channel degradations better. The investigated wireless communication system is the Orthogonal Frequency Division Multiplexing system with channel equalization. The simulation results reveal the success of the proposed work for robust image communication.

Keywords Steganography · DCT · DWT · YD_bD_r · AWGN · OFDM · LSE

1 Introduction

The idea of image steganography is hiding image in another cover image. The objective of any image steganography scheme is to secure some secret images from intruders. Both secret images and the cover image need to be saved from deteriorations. The cover image quality and hidden image secrecy are main targets [1].

Although last image steganography approaches are widely used for securing secret data, they have problems such as capacity or the quality of steganography image or security or

✉ Asmaa Abdelmonem Eyssa
asmaaengineering@yahoo.com

[1] Department of Electronics and Communication Engineering, Faculty of Engineering, Zagazig University, Zagazig, Egypt

[2] Department of Electronics and Electrical Communication, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

noise. Different approaches have been presented for image steganography based on spatial and transformed domains such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [2]. Hussain et al. presented a survey on spatial domain techniques implementing Least Significant Bit (LSB) approaches [3]. Sandoval et al. presented a spatial domain image steganography method by embedding data in pixel values directly [4]. This method is subjected to removal of the secret image through simple manipulations such as filters. Sheidaee et al. presented DCT steganography approach, whose basic idea is to embed data in DCT lowest and medium coefficients [5]. Kim et al. performed image steganography based on block matching in DWT [6]. Steganography approaches have been studied in the literature without consideration of the wireless communication segment. With the modern advances in communication systems and the bad need to secure images through the communication process, there is a necessity to investigate the robustness of the steganography process in the presence of communication channel degradations. OFDM is the most widely used wireless communication technology. OFDM doesn't need complex equalization filters. It uses many slowly modulated narrowband signals rather than the rapidly modulated wideband signal. Therefore, the channel equalization is simplified so that they are considered as the advantages of OFDM. OFDM presents low symbol rate, which makes a guard interval between symbols, and also it has the capability to eliminate Inter-Symbol Interference (ISI), echoes, and time-spreading [7–9]. This work is divided into two parts, The objective of the first part is performing steganography approach, which achieves high security and high capacity with keeping the quality of steganography image. The objective of the second part is studying the effect of channels through OFDM on this proposed approach.

2 Related Work

Most of the researches carried out in the area of image steganography depend on DCT, DWT, and the LSB. This part offers the latest methods for hiding data in a cover image. In [10], the researchers used Advanced Encryption Standard (AES) encryption algorithm on a secret image in order to increase safety. In order to embed secret image, IWT, and LSB are used after dividing the host image into blocks. Due to using blocks, there is a little distortion in the steganography image. If there is an increase in the size of the data, the distortion will be clear in the steganography image. In [11], the proposed method depends on DCT. At the first,the authors used filter to determine the position of the edges of color image, so they used limited size of data. After that performing DCT on (Red, Green, Blue) channels of the image. The half difference of coefficients of (Red, Blue) represents 0 and a half average of coefficients of (Red, Blue) represents 1 from embedded data. After that, they put them in an equal position of green coefficients. If there is noise, the positions of edges will be changed and the extracted data will be deformed.

In [12], the authors used an image scrambling in order to preserve the privacy of image contents, after that it's converted to an un correlated color space HSV. On the other hand, an Iterative Magic Matrix Encryption Algorithm (IMMEA) encrypts the secret data. In order to embed data into V plane of HSV color model, LSB method is used. This way gives high quality for steganography images with low capacity because it used one plane of HSV color model. In [13], the researchers implemented image steganography by embedding message to LSB of quantized DCT coefficients which is performed on YC_bC_r components of cover image. In [14], the authors used fuzzy edge detection in order to detect the edges of image for embedding

secret data in it by LSB method. this method gives high quality. The idea of the technique in [15] is embedding encrypted secret text into 2D Haar Discrete Wavelet Transform coefficients of YC_bC_r model channels. Despite getting high PSNR, the size of secret data is small. The method in [16] allows embedding of three secret images in the RGB color coordinate system using DWT. Secret images and cover image are divided into four bands by DWT and embeds LL bands of color plans of secret images into three color plans of cover image.

The previously mentioned approaches and some others used spatial domain and frequency domain with properties of the cover image. The enhancement of data security maintains the quality of the steganography and secret images. In this study, image steganography used an uncorrelated color space, DWT, DCT, and chaotic Baker map encryption are adopted to achieve security. The second part of this paper presents transmitting steganography image through OFDM over wireless channels and study their effects on the reconstructed images.

3 The Proposed Algorithm of Image Steganography

The first part of this research proposes a new technique. The proposed technique is divided into two algorithms (Embedding and Extracting). We have used encryption, DCT and DWT inorder to make it more secure.

3.1 Embedding of Secret Images

It illustrates how to hide three secret images in the cover image as shown in Fig. 1. The cover image size is chosen to be (512×512). The payload images have equal size (256×256) because the size of each band from DWT on the cover image is (256×256), It is necessary to perform encryption to increase security. This proposed algorithm used high frequency bands (LH, HL, HH),so we can embed three secret images with size (256×256) in these bands.

Step 1 Chaotic Backer map encryption is used for changing the order of pixels of secret images with a key. It's used with DCT to prevent any attacker from knowing secret data.
Step 2 The red, blue, and green components of both the cover and encrypted secret images are separated.
Step 3 The red, blue and green components are normalized to a maximum of 1.
Step 4 Normalized components (Rn,Gn,Bn) are converted to Y,D_b,D_r components in order to increase the security.
Step 5 DWT is performed on each of the normalized components of the cover image and DCT performed on each of the RGB normalized component of the secret images.
Step 6 Gain coefficient (α_1) is multiplied by DCT coefficients of each normalized channel of RGB model for each secret image. DWT coefficients in (LH,HL,HH) bands for each channel of YD_bD_r color model of the cover image are combined with DCT coefficients of the normalized channels of RGB model of each secret image. $M(x, y) = C(x, y) + \alpha_1 P(x, y)$,where M is considered to be DWT coefficients of each component of YD_bD_r color model of modified cover image, C is DWT coefficients of (LH "Vertical details", HL" horizontal details ",HH "diagonal details") bands for every channel YD_bD_r of original cover image, P is DCT of normalized channels of RGB model for each payload image, α_1 is chosen in such a way that the payload images are not visible in the steganography image.

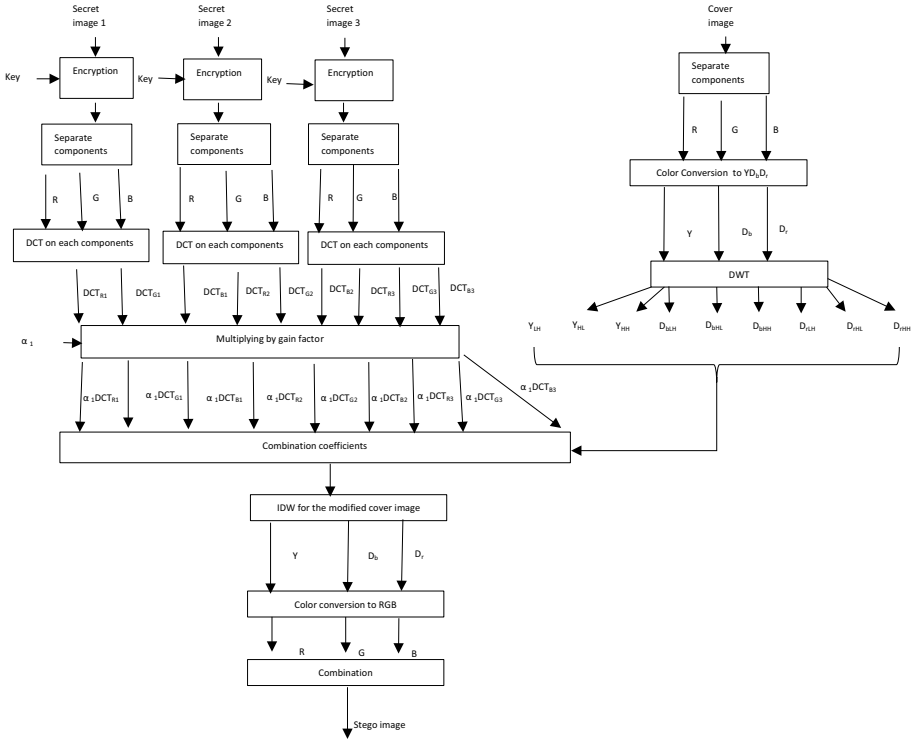


Fig. 1 Embedding model

Step 7 Inverse DWT is performed on each channel resulting from the combination.
Step 8 "YD_bD_r" is converted to RGB on results from step 7 to get a steganography image.

3.2 Extracting of Secret Images

The extracting algorithm explains how to extract three secret images from steganography image by knowing the cover image at the receiver as shown in Fig. 2.

Step 1 Red, Blue and Green components of both the steganography and cover images are separated.
Step 2 All the three components in both cases are normalized.
Step 3 The normalized channels are converted to "YD_bD_r" channels.
Step 4 2-D DWT is performed on components resulting from step 3 on cover and steganography images using DWT.
Step 5 The difference between high coefficients bands of DWT(LH "Vertical details", HL" horizontal details ",HH "diagonal details") for each channel of steganography and cover images is performed. Inverse DCT is computed for difference components for each channel coefficients.
Step 6 RGB components resulting from step 5 are combined inorder to get the extracted encrypted secret images.

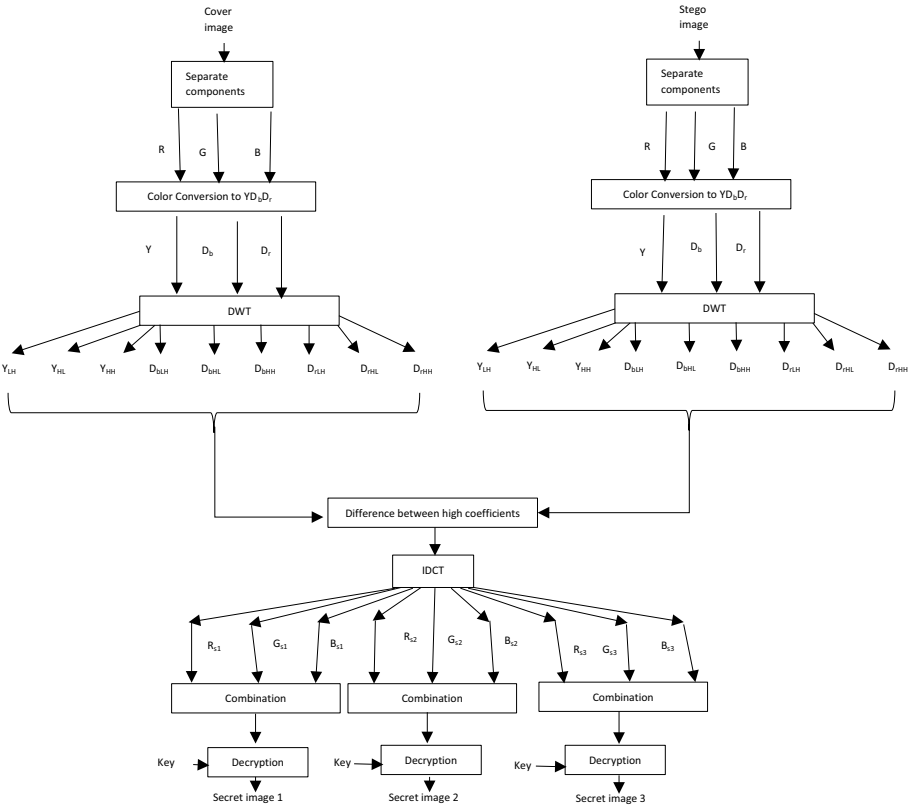


Fig. 2 Extracting model

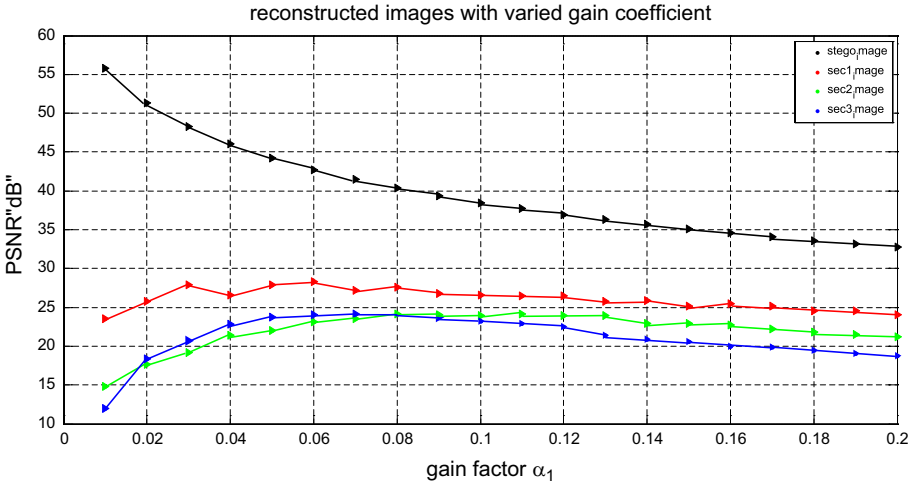


Fig. 3 The effect of changing gain factor on steganography images

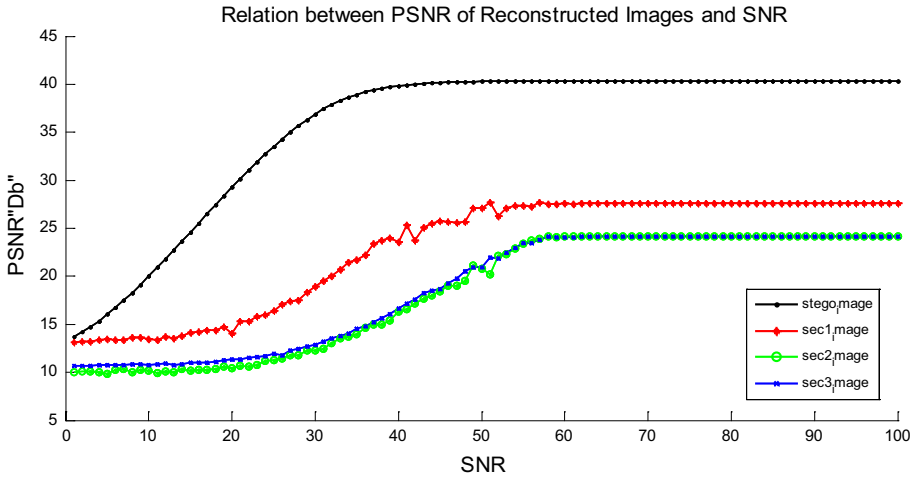


Fig. 4 Reconstructed images with AWGN

Step 7 The chaotic Backer map decryption with the key is performed to get the extracted images.

3.3 Analysis to Get Values of α_1

By obtaining the relation between α_1 and PSNR for all reconstructed images as shown in the curve found in Fig. 3. The Peak Signal to Noise Ratio (PSNR (dB)) is one of the public matrices for evaluating the quality of images. It's clear from the curve, 0.08 is the best value of α_1 inorder to get the best PSNR for all reconstructed image.

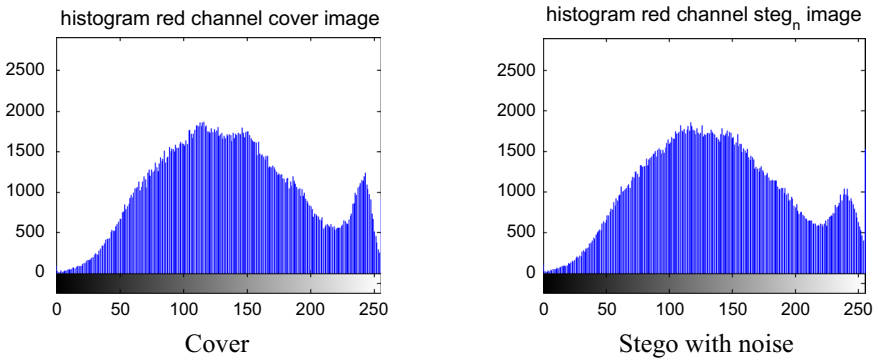
3.4 Stego Image with an Additive White Gaussian Noise

If we add white Gaussian noise to the stego image, where the range of SNR from (1 to 100). It's observed that the curve in Fig. 4 has a good PSNR at $\alpha_1 = 0.08$ for all reconstructed image. Stego image has a good quality at noise as shown in Fig. 5. Figure 6 shows the reconstructed images at SNR = 30 dB.

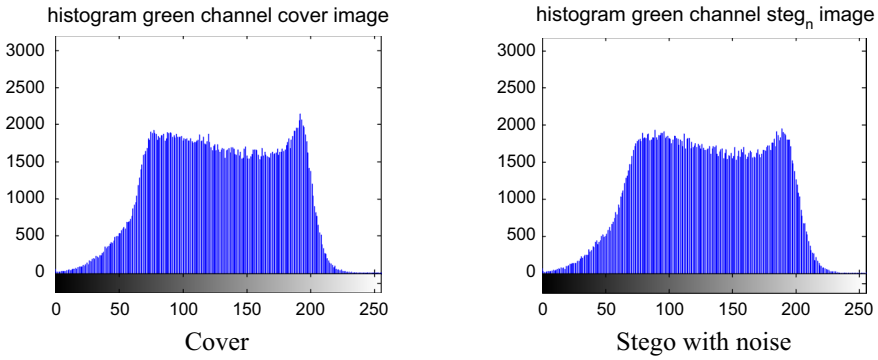
4 Transmitting Steganography Image in OFDM with Gaussian and Rayleigh Fading Channels

4.1 Transmitting Steganography Image Through OFDM

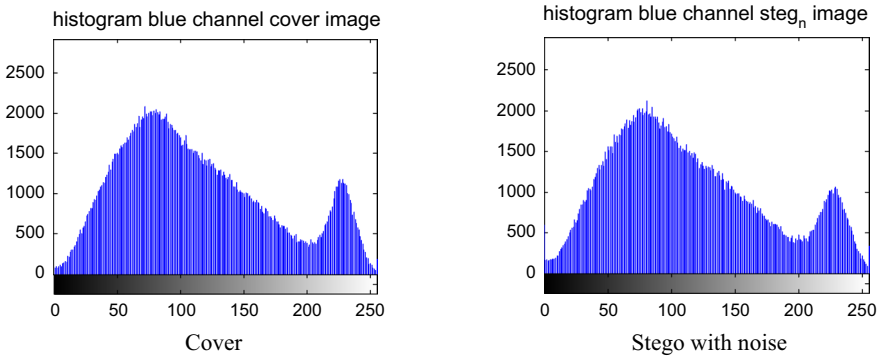
- Figure 7 illustrates OFDM system where the input is steganography image obtained from the embedding algorithm.



(a) Histogram for Red channel noisy stego image at SNR=30 dB compared to the cover image.



(b) Histogram for green channel noisy stego image at SNR=30 dB compared to the cover image.



(c) Histogram for blue channel noisy stego image at SNR=30 dB compared to the cover image.

Fig. 5 **a**, **b**, **c** Histogram for red, green and blue channel for noisy stego image at SNR = 30 dB compared to the cover image. (Color figure online)

- In OFDM modulation block, we used Quadrature Amplitude Modulation QAM with order 2. High efficiency is resulted from utilizing QAM obtained by setting a suitable constellation size in order to match the noise level of the communications channel.

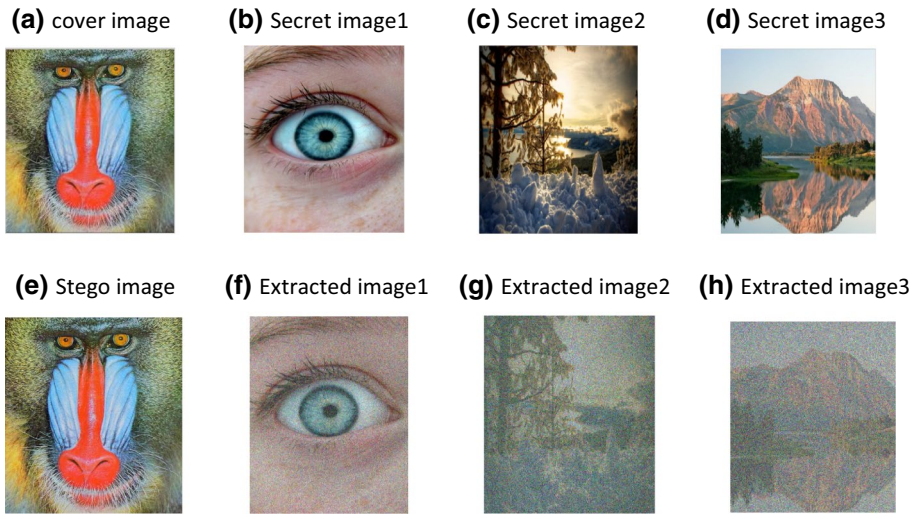


Fig. 6 Reconstructed images at $\alpha_1 = 0.08$ with noise at SNR = 30 dB

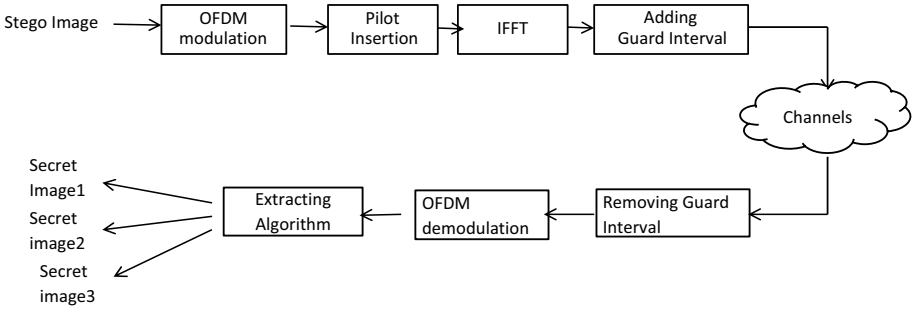


Fig. 7 OFDM transmit model for steganography image

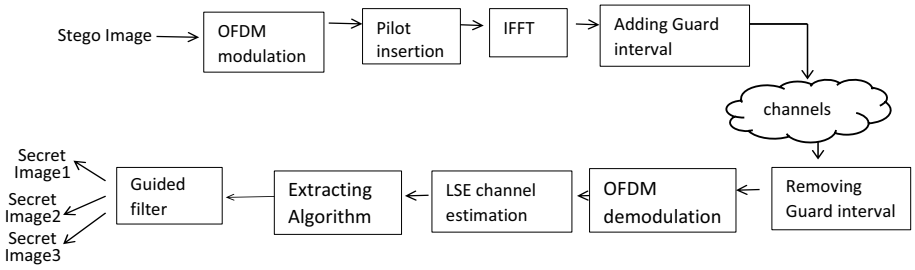


Fig. 8 OFDM transmitting model with modification for stego image

- The pilot symbol is transmitted with the received signal to detect the OFDM symbol start. It can also be used for channel estimation. Sam in [17] used pilot symbols for analysing and implementation of channel estimation in OFDM system, where the pilot

symbol has a special symmetry so that the pilot symbol doesn't need to be known at the receiver.
- The IFFT block computes Inverse Fast Fourier Transform for high-efficiency signal processing.
- One of the solutions to overcome the Rayleigh channel effect is using OFDM with a Guard Interval (GI) [18], because it resists propagation delays, and reduces interference to the next user.

4.2 Transmitting Steganography Image in OFDM with Modification

Figure 8 illustrates the modified OFDM system, it utilizes Least Square estimation channel (LSE). These fading profiles introduce inter-symbol interference, it must be compensated by using channel estimation to enhance the quality of steganography image. After that, guided image filter has been used. The content of a guidance image is utilized by the guided filter to make filtering on a specific image, which can be the input image itself or another different image. The guided filter is based on an edge preserving smoothing operator. The guided filter is widely performed in a great variety of computer vision and computer graphics applications because of its noise reduction, detail smoothing/enhancement [19]. The modification in the receiving side of OFDM has been introduced in order to enhance the performance of OFDM system on transmitted image over wireless channels.

5 Results and Discussion

Table 1 shows results at Rayleigh fading and AWGN channels at delays = [0,1e09], Gain = [0,0], SNR = 30 dB, and size of steganography _color image is 512×512. It's clear that the AWGN and Multipath Fading channels have a very bad effect on transmitting steganography image through OFDM system. Due to these channels, the steganography image will have noise and the value of pixels will be changed, then the steganography and the secret image will be destroied. The correlation coefficient represents the performance of steganography image through OFDM, where a higher correlation coefficient means that the reconstructed images have a high quality. As a result of bad outputs, the OFDM system must be modified to get better results and enhances the quality of reconstructed images. So, channel estimation and filter are used to compensate the errors resulting from wireless channels. Correlation coefficients for reconstructed images obtained from the modified OFDM are listed in Table 2. The correlation coefficient equals 1 when there is no change in the image. From Fig. 9, it is clear that using LS channel estimation gives a good quality for reconstructed images. And also Table 3 shows the Doppler Effect on reconstructed images through OFDM with modification. Despite the noise generated by AWGN and Rayleigh channels, the quality of reconstructed images is good at different Doppler shift values at SNR = 30 dB. The algorithm that's found in [10] embeds data in LSB

Table 1 Correlation coefficients for reconstructed images in OFDM

Reconstructed images	Steganography image	Secret image1	Secret image2	Secret image3
Correlation coefficient	Red channel = 0.0074	Red channel = 1.4751e−04	Red channel = 0.0017	Red channel = 0.0063
	Green channel = − 0.0095	Green channel = − 0.0062	Green channel = − 0.0029	Green channel = − 0.0064
	Blue channel = 0.0077	Blue channel = − 0.0074	Blue channel = − 0.0015	Blue channel = − 0.0078

Table 2 Correlation coefficients for reconstructed images in modified OFDM

Reconstructed images	Steganography image	Secret image1	Secret image2	Secret image3
Correlation coefficient with LSE at SNR = 20	Red channel = 0.9682	Red channel = 0.6925	Red channel = 0.5339	Red channel = 0.4608
	Green channel = 0.9754	Green channel = 0.6377	Green channel = 0.4351	Green channel = 0.3817
	Blue channel = 0.9502	Blue channel = 0.6324	Blue channel = 0.3806	Blue channel = 0.4318
Correlation coefficient with LSE at SNR = 30	Red channel = 0.9966	Red channel = 0.9637	Red channel = 0.8828	Red channel = 0.8250
	Green channel = 0.9978	Green channel = 0.9578	Green channel = 0.8595	Green channel = 0.8297
	Blue channel = 0.9950	Blue channel = 0.9571	Blue channel = 0.8294	Blue channel = 0.8761
Correlation coefficient with LSE at SNR = 40	Red channel = 0.9996	Red channel = 0.9912	Red channel = 0.9738	Red channel = 0.9745
	Green channel = 0.9999	Green channel = 0.9885	Green channel = 0.9753	Green channel = 0.9746
	Blue channel = 0.9990	Blue channel = 0.9883	Blue channel = 0.9687	Blue channel = 0.9801

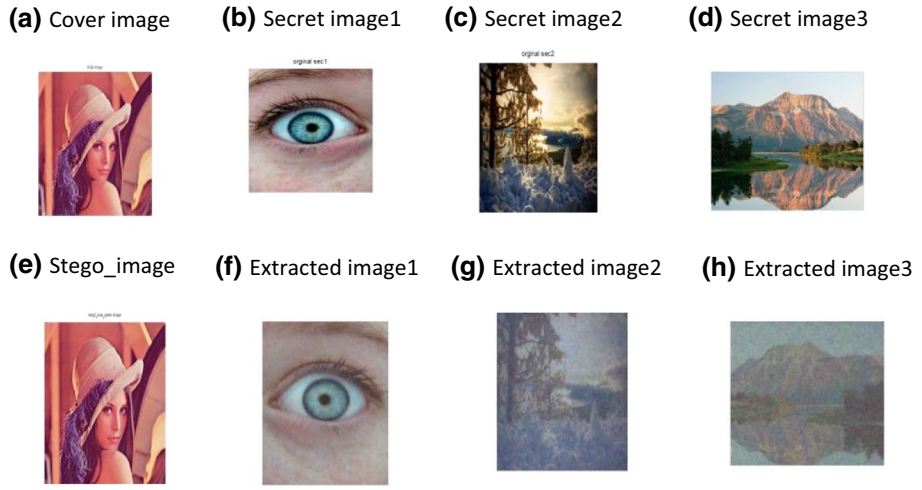


Fig. 9 Reconstructed images at SNR = 30 dB and Rayleigh channel

of high coefficients of IWT of the blocked cover image, The quality deteriorates if the size of the secret image further increases, The algorithm in [12],when the percentage of secret data becomes 72,74% the PSNR of stego image will be 21.96. The idea of this algorithm is embedding data in LSB of V plane of HSV conversion of an encrypted cover image. Despite the highest PSNR, the capacity of secret data is low. The algorithm found in [13] depends on the properties of cover image YC_bC_r, the embedding process based on LSB technique with DCT transform. The capacity is low with small PSNR.In this proposed approach the capacity percentage of secret data is 75% compared with the latest algorithms found in Table 4. The proposed approach of steganography enables us to embed the highest capacity of secret data, where the capacity is the number of bits that can be embedded in cover media. Additionally using color space YD_bD_r gives high quality and high security compared to others color spaces models as shown in Table 5. From Fig. 10,it's clear that BER gotten from OFDM system modification is satisfied compared with transmitting the image over AWGN channel in methods [10]. As shown in Fig. 11, it's clear that OFDM with modification gives the lowest BER compared with OFDM without modification over AWGN and Rayleigh channels.

Table 3 Reconstructed images at different Doppler shift over A WGN and Rayleigh channels

Reconstructed Images	Steganography Image	Secret image1	Secret image2	Secret image3
Correlation coefficient with LSE at Doppler = 0.1	Red channel = 0.9965	Red channel = 0.8355	Red channel = 0.7190	Red channel = 0.5713
	Green channel = 0.9977	Green channel = 0.8403	Green channel = 0.7274	Green channel = 0.6258
	Blue channel = 0.9959	Blue channel = 0.8420	Blue channel = 0.6776	Blue channel = 0.6690
Correlation coefficient with LSE at Doppler = 0.5	Red channel = 0.9965	Red channel = 0.8235	Red channel = 0.6983	Red channel = 0.5712
	Green channel = 0.9975	Green channel = 0.8359	Green channel = 0.6886	Green channel = 0.6244
	Blue channel = 0.9948	Blue channel = 0.8371	Blue channel = 0.6365	Blue channel = 0.6698
Correlation coefficient with LSE at Doppler = 0.9	Red channel = 0.9971	Red channel = 0.8149	Red channel = 0.6425	Red channel = 0.5791
	Green channel = 0.9972	Green channel = 0.8274	Green channel = 0.6628	Green channel = 0.6371
	Blue channel = 0.9928	Blue channel = 0.8298	Blue channel = 0.6118	Blue channel = 0.6759

Table 4 Comparison between capacity of last methods and the proposed approach

Schemes	PSNR (*dB*) of steganography image	Percentage of capacity
Scheme [10]	21.96	72.74
Scheme [12]	56	1.04
Scheme [13]	36.882	1.05
proposed algorithm	40.4615	75

Table 5 Effect of uncorrelated color spaces on reconstructed images

Color space model	Stego image	Secret image1	Secret image2	Secret image3
RGB	14.3945	14.6753	10.7607	11.8981
YC_BC_R	34.6146	29.0752	23.7501	20.9739
UVL	28.8035	19.3065	6.9845	15.9070
HSV	21.1425	13.4484	11.0832	11.3991
YIQ	37.3343	28.1615	23.7933	25.3329
YD_bD_r	40.3142	28.0156	23.9165	24.2475

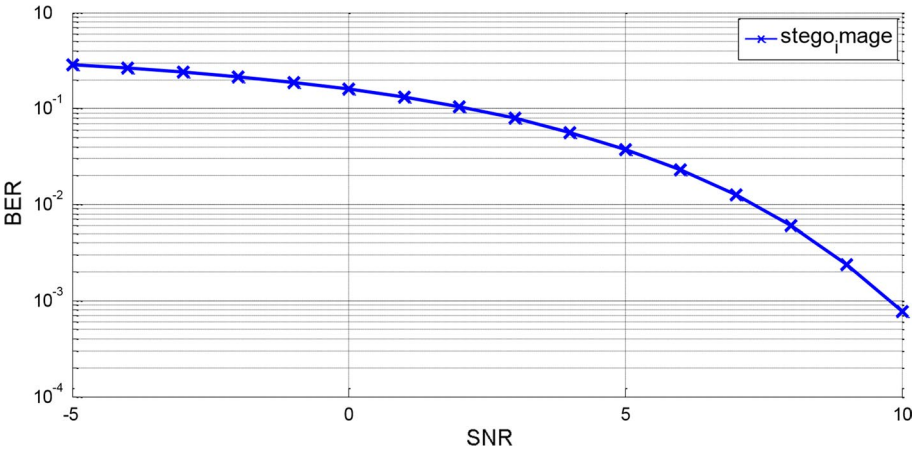


Fig. 10 BER of steganography image over AWGN channel

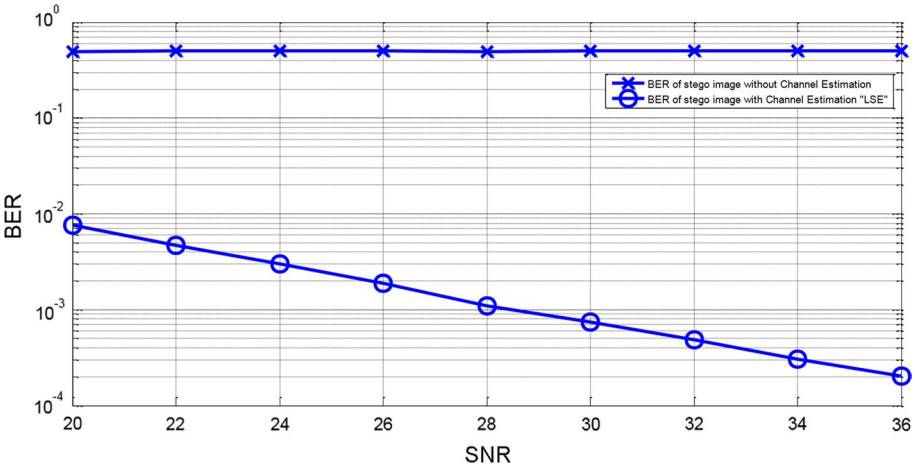


Fig. 11 Comparison between BER of transmitting steganography images through OFDM and OFDM with modification over AWGN and Rayleigh channels

6 Conclusion

This paper has introduced an efficient approach for embedding and extracting steganography data, and also the proposed approach enables us to hide three images in one cover image. It also achieves more security because of using a gain coefficient (α_1), merging two different types of image transforms and encryption. In this paper, the effect of AWGN and multipath fading channels on the steganography image and the extracted data through OFDM system has been studied. In order to reduce the distortion resulted from wireless channels, the modification on OFDM system has been performed. Simulation results are promising towards a more efficient colour steganography scheme.

References

1. Tripathi, D., & Sharma, S. (2016). A robust 3-SWT multiple image steganography and contrast enhancement technique. In *2016 International conference on inventive computation technologies (ICICT)*, Coimbatore, 2016 (pp. 1–6).
2. Malathi, P., & Gireeshkumar, T. (2016). Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains. *Procedia Computer Science, 93,* 878–885.
3. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. S., & Jung, K.-H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65,* 46–66.
4. Sandoval, O. J., Hernandez, M. C., Miyatake, M. N., Meana, H. P., & Toscano, K. (2016). MedinaImageadaptive steganalysis for LSB matching steganography. In *2016 39th international conference on telecommunications and signal processing (TSP)* (pp. 478–483).

5. Sheidaee, A., & Farzinvash, L. (2017). A novel image steganography method based on DCT and LSB. In *2017 9th International conference on Information and Knowledge Technology (IKT)*, Tehran (pp. 116–123).
6. Kim, J., Park, H., & Park, J. (2017). Image steganography based on block matching in DWT domain. In *2017 IEEE international symposium on broadband multimedia systems and broadcasting (BMSB)*, Cagliari (pp. 1–4).
7. Tiwari, R., Pathak, A., & Mishra, R. (2014). A study on steganography image. *Journal of Science, Engineering and Technology Research (IJSETR), 3*(10).
8. Hariprasad, N., & Sundari, G. (2015). Comparative analysis of the BER performance of DWT OFDM over that of FFT OFDM in presence of phase noise. In *2015 International conference on robotics, automation, control and embedded systems (RACE),* Chennai (pp. 1–4).
9. Wang, Zhongpeng, Chen, Fangni, Qiu, Weiwei, Chen, Shoufa, & Ren, Dongxiao. (2018). A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission. *Optics Communications, 410,* 94–101.
10. Seethalakshmi, K. S., Usha, B. A., & Sangeetha, K. N. (2016). Security enhancement in image steganography using neural networks and visual cryptography. In *2016 International conference on computation system and information technology for sustainable solutions (CSITSS), IEEE conference publications* (pp. 396–403).
11. Lahiri, S., Paul, P., Banerjee, S., Mitra, S., Mukhopadhyay, A., & Gangopadhyaya, M. (2016). Image steganography on coloured images using edge based Data Hiding in DCT domain. In *2016 IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON)* (pp. 1–8).
12. Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems* (in press, Corrected Proof, Available online 27 November 2016).
13. El Rahman, S. A. (2016). A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. *Computers and Electrical Engineering* (Available online 19 September 2016).
14. Dadgostar, H., & Afsari, F. (2016). Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. *Journal of Information Security and Applications, 30,* 94–104.
15. Broda, M., Hajduk, V., & Levický, D. (2015). Image steganography based on combination of YCb-Crcolor model and DWT. In *2015 57th international symposium ELMAR (ELMAR)*, Zadar (pp. 201–204).
16. Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. In *International conference on information and communication technologies (ICICT 2014)*.
17. Sam, J. A., & Nair, A. K. (2016). Analysis and implementation of channel estimation in OFDM system using pilot symbols. In *2016 International conference on control, instrumentation, communication and computational technologies (ICCICCT)*, Kumaracoil (pp. 725–728).
18. Odarchenko, R., Tkalich, O., Shevchuk, Z., & Lukin, S. (2015). OFDM signal formation with adaptive guard interval duration change. In *2015 Second international scientific-practical conference problems of infocommunications science and technology (PIC S&T)*, Kharkiv (pp. 216–219).
19. Jia, Y., Rong, C., Wu, C., & Yang, Y. (2017). Research on the decomposition and fusion method for the infrared and visible images based on the guided image filtering and Gaussian filter. In *2017 3rd IEEE international conference on computer and communications (ICCC)*, Chengdu (pp. 1797–1802).
20. Mannan, A., & Habib, A. (2017). Adaptive processing of image using DWT and FFT OFDM in AWGN and Rayleigh channel. In *2017 International conference on communication, computing and digital systems (C-CODE)*, Islamabad (pp. 346–350).

Asmaa Abdelmonem Eyssa is M.Sc. in Faculty of Engineering at Zagazig University, she is interested in steganography, watermarking and encryption areas, she is interested in wireless communication systems.

Fathi Elsaid Abdelsamie is a professor in Faculty of Engineering at Menouf University, his interest in steganography, watermarking and encryption areas, he is interested in wireless communication systems.

Abdelaziz Elsaid Abdelnaiem is a professor in Faculty of Engineering at Zagazig University, his interest in steganography, watermarking and encryption areas, she is interested in wireless communication systems.