HIGHER LEVEL SECURITY APPROACH FOR DATA COMMUNICATION SYSTEM BASED ON AES CRYPTOGRAPHY AND DWT STEGANOGRAPHY

Saja M. Saraireh[1] and Aser M. Matarneh[2]

Department of Electrical Engineering, Mutah University, Jordan
aser_m2002@yahoo.com[2], aser.matarneh@mutah.edu.jo[2]

(Received: 27-Mar.-2016, Revised: 23-Jun.-2016, Accepted: 26-Jun.-2016)

ABSTRACT

Cryptography is used for secured data transmission, but the resulting unreadable messages usually attract other's attention, so steganography is employed to hide the secret information to prevent attackers from discovering the presence of secret data. This paper proposes an improved technique that combines both Advanced Encryption Standard (AES) algorithm for cryptography and steganography and takes the advantages of using the high frequency coefficients of the cover image by applying the Discrete Wavelet Transform (DWT).The proposed technique is employed to study the effect of hiding the encrypted secret message in 24-bit RGB image. The performance of the proposed method is evaluated in terms of the Peak Signal to Noise Ratio (PSNR) analysis, the payload embedding capacity and the histogram distribution analysis. Comparison to other four associated works will be offered. Experimental results reveal that the proposed method gives a secure technique for data hiding and shows robustness against different attacks.

KEYWORDS

DWT, Steganography, AES, Cryptography, PSNR, Payload, Histogram.

1. INTRODUCTION

Security problems become an essential issue due to exchanging large amounts of data on computer networks [1]. This has resulted in the appearance of a lot of applications that are concerned with the data hiding field, such as; cryptography, watermarking, fingerprinting and steganography. The most two preferred techniques are cryptography and steganography [2]-[3]. Although these two are related, there is a difference between them; cryptography encrypts the secret text, but its presence is still detectable, so that the message can be intercepted and altered by the attacker. In contrast, steganography conceals the existence of the secret data in another medium [4]-[5], so that the development of steganography provides secure transfer of data without stimulating any doubt, where different techniques for data hiding are used to hide the secret data into a cover medium [6]-[7].

Steganography methods are classified into; spatial domain-based steganography and frequency domain-based steganography [8]. Spatial domain techniques use the pixel's least significant bits (LSBs) to embed the secret message bits. The resulting stego-image is susceptible to many noisy operations because of the simplicity of LSB techniques [9]. Frequency domain techniques utilize the properties of the cover image and then the steganography robustness is improved [5].

There have been a lot of works using the combination of both cryptography and steganography or one of them. In [10], DWT is used to embed the secret message in a gray image. It provides high stego-image quality although it embeds large capacity of data. In [11], DWT steganography method was used, in which the data is hidden in the main components of the sub-image. These are; the horizontal, the vertical and the diagonal components.

In [12], a method was presented that uses a combined application of steganography and visual cryptography. It provides the protection for the customer identity, then a limited amount of information is given for money transfer through the shopping on internet. In [13], AES Rijndeal method and secret key steganography are combined to provide higher security and higher hidden data rate. In AES, the message is powerfully encrypted. By steganography, Discrete Cosine Transform (DCT) of an image is used, where two secret keys are generated in such a manner that makes the system highly secured. In [14], a symmetric key RSA and symmetric key AES algorithms are employed to encrypt the data, then LSB steganography technique is used to embed the encrypted data into the cover image. A combination of RSA algorithm and DCT with LSB technique is proposed in [15], where the message is encrypted using RSA, then embedded using DCT with LSB in digital media. Custom neural network is used for extracting the encrypted data.

The main aim of AES encryption/decryption process integrated with steganography is to offer a high level of security with moderate capacity albeit the complexity added by such model. The system would become robust against attacks if the security issue is properly tackled.

The proposed algorithm is based on DWT using colored digital images and AES encryption techniques, whereas the similar algorithm has been proposed in [16] for gray images based on Double Density Dual Tree (DD DT) DWT using AES and T-codes. However, although the proposed algorithm in [16] offers a higher degree of security, the quality of the stego-image is still a critical issue.

In this paper, the advanced encrypted standard (AES) cryptography technique is employed to encrypt the secret message, and (DWT) steganography is used to embed the encrypted secret message in the cover image, with utilizing the advantages of 24-bit RGB image as it is a cover medium and using the pixel indicator technique (PIT) to embed the encrypted secret message in the cover image which is proposed in [17]. The proposed method is evaluated by comparing it to other four methods. It achieves higher Peak Signal to Noise Ratio (PSNR) values and makes a trade-off between capacity and security. The rest of the paper is organized as follows; in section 2 the proposed system is introduced, while section 3 presents and discusses the experimental results and then, the paper is concluded in section 4.

2. PROPOSED SYSTEM

The main idea of the proposed algorithm is to combine both AES cryptography and DWT steganography, with utilizing the advantages of 24-bit RGB images by using PIT. Next sub-sections briefly introduce these techniques.

2.1 Two-Dimensional Haar-DWT

The operations of the two-dimensional Haar-DWT result of four different sub-bands are denoted as LL, HL, LH and HH, as shown in Figure 1. These four sub-bands represent four sub-images of the same size (M/2, N/2) that are obtained from an image of size (M, N) [9, 19], as shown in Figure 2. Some information is obtained from these sub-bands (LL, HL, LH, HH), since the cover image pixels are classified into less important and more important pixels [5]. According to this, the LL sub-band is not used for embedding, since it contains vital information about the original image, and any changes in it will affect the quality of the image and can be easily noticed by the human eye [20].

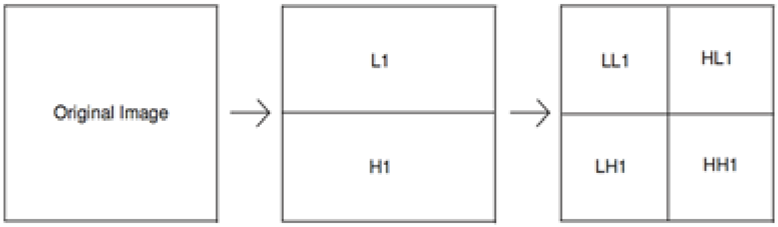

Figure 1. The horizontal operation and the vertical operation of DWT.

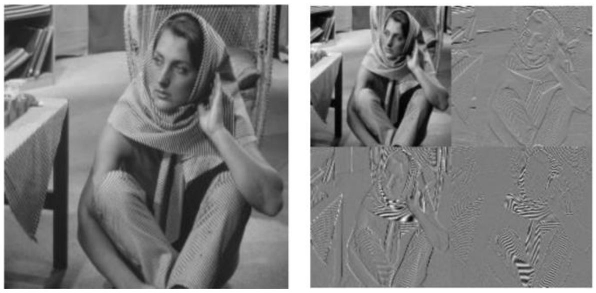

Figure 2. The original image to the left and its DWT to the right.

2.2 Pixel Indicator Technique (PIT)

Pixel indicator technique was used for 24-bit RGB image steganography. The RGB channels of the image are classified by this technique to be: the indicator, channel 1 and channel 2 in specified order. The 2 LSBs of the indicator channel are used to specify the embedding of data in channel 1 and channel 2 [17]. Table 1 shows this technique. An improvement on this technique is proposed in [20], where instead of embedding only 2 bits in the channel selected for the embedding, (1, 2 or 3) bits can be embedded in that channel according to the number of zeros in the most significant part MSB, where 1 bit is embedded if the number of zeros in the MSB is 0 or 4, 2 bits are embedded if the number of zeros in the MSB is 2 and 3 bits are embedded if the number of zeros in the MSB is 1 or 3, as shown in Table 2. The proposed technique employs this method in the transform domain instead of using it in the spatial domain to improve security.

2.3 The Embedding Process

As the proposed technique idea is derived from [17] and [21], some improvements should be mentioned, where instead of embedding the secret text clearly, it is embedded after encrypting it by the AES algorithm, then as an alternative of using the spatial domain of the cover image for hiding, the transform domain is employed, and finally, the location of the indicator channel is not fixed, where it depends on the transform band used for embedding.

In the proposed algorithm, the cover image is firstly separated into its RGB color components, then the DWT is applied on each component separately. For the secret text message, the first step is to encrypt it by the AES algorithm, and convert it into its binary representation. The next step is to store its length to variable X and in the first 8 pixels of HL band in the Red channel. To improve security by using the PIT method, the indicator channel is variable. The indicators are chosen according to the transform band that is used to embed the encrypted secret text in it. In the HL band, the Red channel is the indicator. Green and Blue are channel one and channel two, respectively. In the LH band, the Green channel is the indicator. Red and Blue are channel one and channel two, respectively. In the HH band, the Blue channel is the indicator. Red is channel one and Green is channel two.

Table 1. The relation between the indicator and other channels [17].

The 2 LSBs of the indicator	**Channel 1 (green channel)**	**Channel 2 (blue channel)**
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	No hidden data
11	2 bits of hidden data	2 bits of hidden data

Table 2. The hiding process [21].

Number of zeros in the MSB	**LSB**			
	b5	**b6**	**b7**	**b8**
0 or 4	×	×	×	✓
2	×	×	✓	✓
1 or 3	×	✓	✓	✓

The embedding process is started from pixel nine in the HL band of the Red channel. The embedding of the encrypted secret message in the selected channel is executed by the hiding process, as shown in Table 2. The sequence of the embedding algorithm is flowcharted in Figure 3. The process is stopped when the secret message is completely embedded. When the embedding process is completed, the inverse discrete wavelet transform (IDWT) is applied for each RGB channel, then the RGB components are combined in order to obtain the stego-image.

2.4 The Extraction Process

The extraction process is flowcharted in Figure 4. When the secret text message is extracted, which is in binary representation, it is converted into its character representation and decrypted by the AES algorithm. The algorithm will stop based on the length of the secret message which is stored in the first 8 bytes of the Red channel in the HL band.

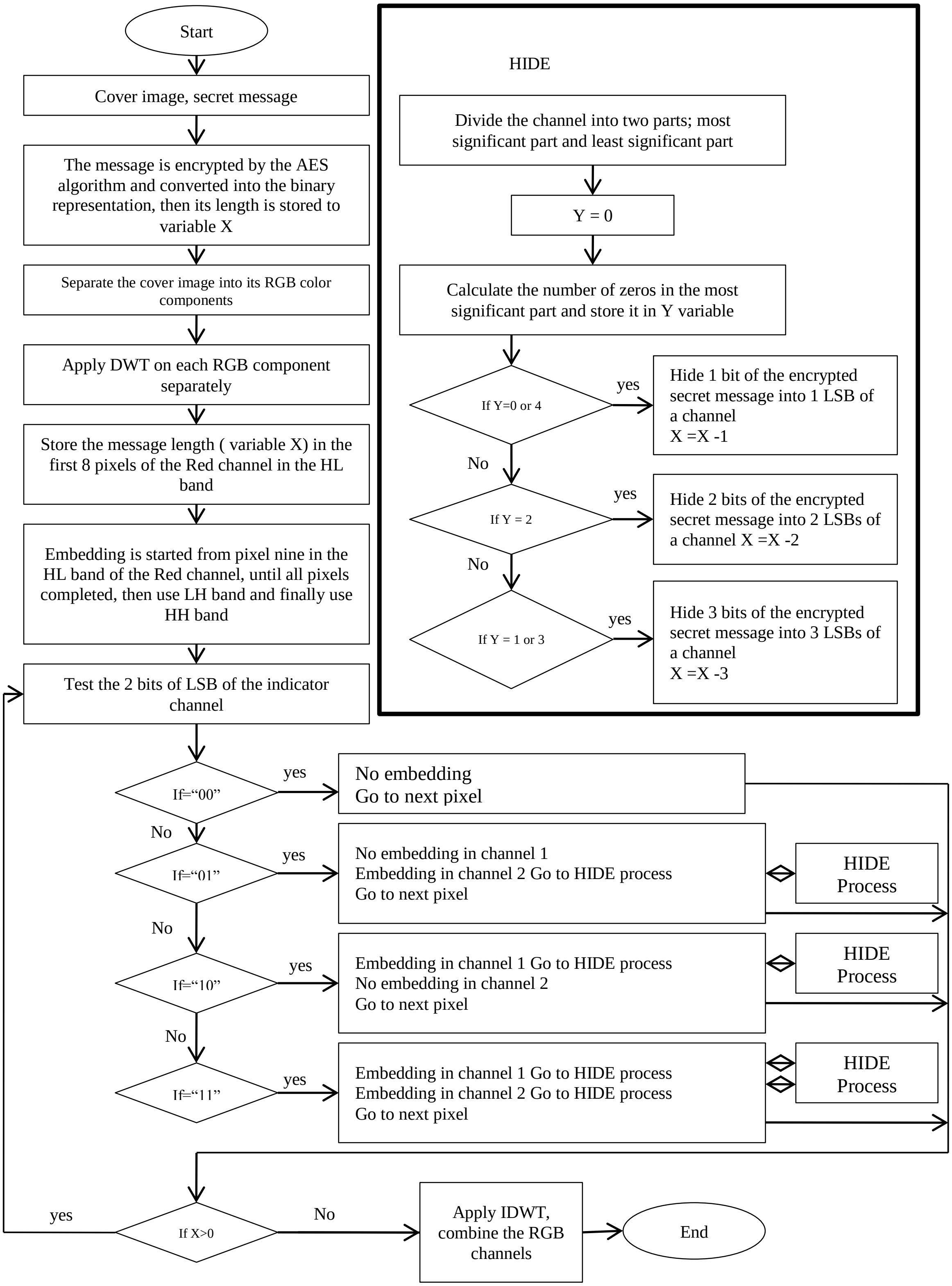
Start
Cover image, secret message
The message is encrypted by the AES algorithm and converted into the binary representation, then its length is stored to variable X
Separate the cover image into its RGB color components
Apply DWT on each RGB component separately
Store the message length (variable X) in the first 8 pixels of the Red channel in the HL band
Embedding is started from pixel nine in the HL band of the Red channel, until all pixels completed, then use LH band and finally use HH band
Test the 2 bits of LSB of the indicator channel
If="00"
yes
No embedding
Go to next pixel
No
If="01"
yes
No embedding in channel 1
Embedding in channel 2 Go to HIDE process
Go to next pixel
HIDE Process
No
If="10"
yes
Embedding in channel 1 Go to HIDE process
No embedding in channel 2
Go to next pixel
HIDE Process
No
If="11"
yes
Embedding in channel 1 Go to HIDE process
Embedding in channel 2 Go to HIDE process
Go to next pixel
HIDE Process
yes
If X>0
No
Apply IDWT, combine the RGB channels
End
HIDE
Divide the channel into two parts; most significant part and least significant part
Y = 0
Calculate the number of zeros in the most significant part and store it in Y variable
If Y=0 or 4
yes
Hide 1 bit of the encrypted secret message into 1 LSB of a channel
X =X -1
No
If Y = 2
yes
Hide 2 bits of the encrypted secret message into 2 LSBs of a channel X =X -2
No
If Y = 1 or 3
yes
Hide 3 bits of the encrypted secret message into 3 LSBs of a channel
X =X -3

Figure 3. The embedding process flowchart.

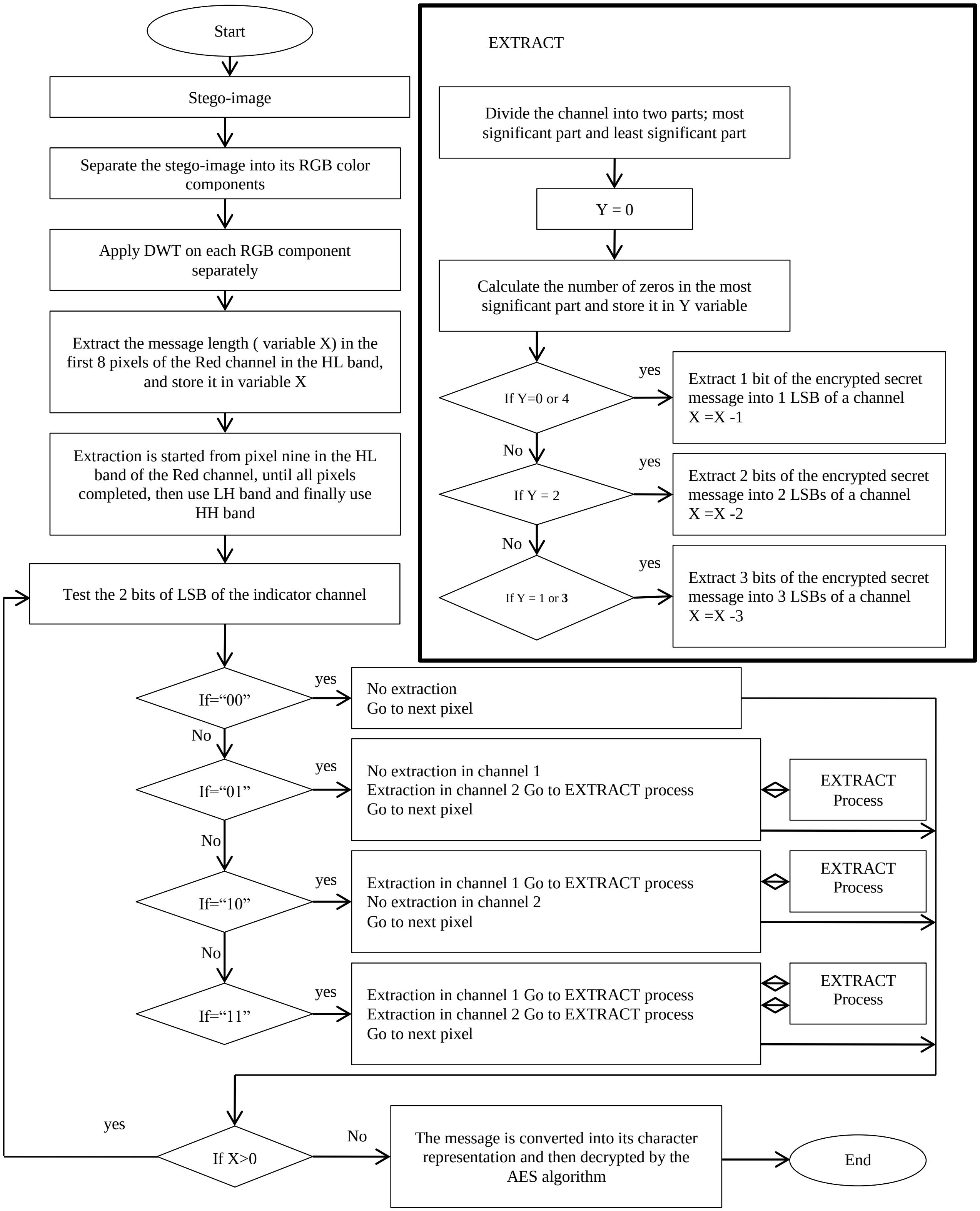
Start
Stego-image
Separate the stego-image into its RGB color components
Apply DWT on each RGB component separately
Extract the message length (variable X) in the first 8 pixels of the Red channel in the HL band, and store it in variable X
Extraction is started from pixel nine in the HL band of the Red channel, until all pixels completed, then use LH band and finally use HH band
Test the 2 bits of LSB of the indicator channel
EXTRACT
Divide the channel into two parts; most significant part and least significant part
Y = 0
Calculate the number of zeros in the most significant part and store it in Y variable
If Y=0 or 4
yes
Extract 1 bit of the encrypted secret message into 1 LSB of a channel
X =X -1
No
If Y = 2
yes
Extract 2 bits of the encrypted secret message into 2 LSBs of a channel
X =X -2
No
If Y = 1 or 3
yes
Extract 3 bits of the encrypted secret message into 3 LSBs of a channel
X =X -3
If="00"
yes
No extraction
Go to next pixel
No
If="01"
yes
No extraction in channel 1
Extraction in channel 2 Go to EXTRACT process
Go to next pixel
EXTRACT Process
No
If="10"
yes
Extraction in channel 1 Go to EXTRACT process
No extraction in channel 2
Go to next pixel
EXTRACT Process
No
If="11"
yes
Extraction in channel 1 Go to EXTRACT process
Extraction in channel 2 Go to EXTRACT process
Go to next pixel
EXTRACT Process
yes
If X>0
No
The message is converted into its character representation and then decrypted by the AES algorithm
End

Figure 4. The extraction process flow chart.

3. Experimental Results

The proposed DWT-based image data hiding technique is implemented using Matlab. To evaluate the performance of the proposed scheme, a number of different types of colored image formats (BMP, JPEG and TIF) are tested. Peak signal to noise ratio PSNR is used for comparing the quality of stego-images with the original images, the payload for embedding capacity and the histogram have been shown to check the degradation of the quality of images. Further, some image processing operations are applied to check robustness. However, the results of only three RGB over images are included in this paper. In addition to that, the effect of increasing the embedded text size on the PSNR and the mean square error MSE is also tested.

The employed images are colored images with a size of 1024×1024x3. Figures (5, 6 and 7) show the original images and the stego-images after embedding an encrypted secret text with a size of 2120 bytes.

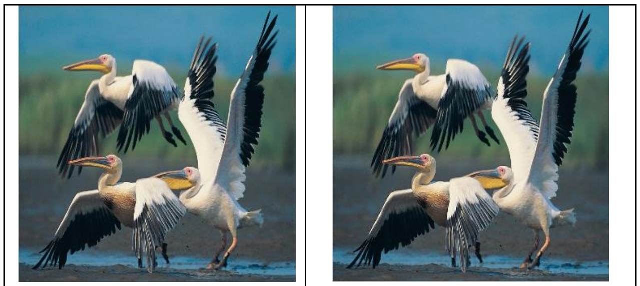

Figure 5. (a) cover-image for (image1) with a size of 1024X1024x3

Figure 5. (b) stego-image for (image1) with a size of 1024X1024x3

Figure 5. (a, b) show cover-image, stego-image after embedding 2120 bytes inside (image 1) picture by the proposed algorithm.

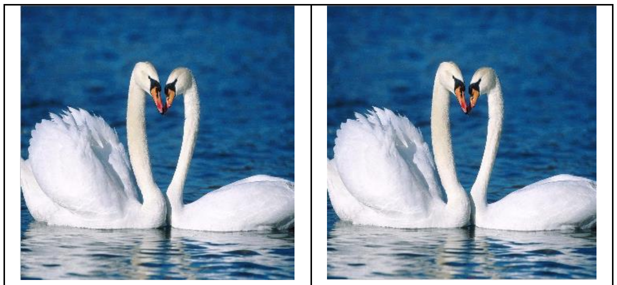

Figure 6. (a) cover-image for (image2) with a size of 1024X1024x3

Figure 6. (b) stego-image for (image2) with a size of 1024X1024x3

Figure 6. (a, b) show cover-image, stego-image after embedding 2120 bytes inside (image 2) picture by the proposed algorithm.

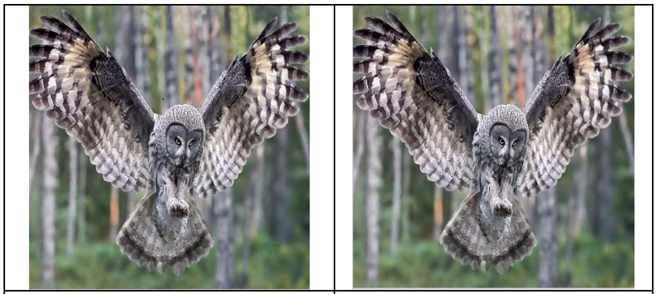

Figure 7. (a) cover-image for (image3) with a size of 1024X1024x3

Figure 7. (b) stego-image for (image3) with a size of 1024X1024x3

Figure 7. (a, b) show cover-image, stego-image after embedding 2120 bytes inside (image 3) picture by the proposed algorithm.

The stego-images are looking intact, which means that the proposed algorithm provides high quality of the stego-image. This can be measured with some tests. The PSNR test measures the image quality by comparing the original image with the stego-image. PSNR can be obtained using Equation 1 [22]. As a high level of security can be obtained for high PSNR values, the human eye will not be able to discriminate between the original image and the stego-image, because the stego-image will be very similar to the original cover image and the attacker would not detect the hidden information. The PSNR values of the proposed system for different images are summarized in Table 3, including a comparison with other ones that use 24-bit color images ([17] and [21]), which are described briefly in section 2.3, in addition to [23] which includes an embedding process that depends on calculating the number of zeros and ones in the (red) indicator channel, then obtaining the absolute difference between them. The resulting value is used to determine the number of bits that should be embedded in channel 1 and channel 2, as well as another technique called simple DWT-based steganography, which embeds one bit of the secret text on each LSB of the pixels in the high frequency bands (HL, LH, HH) of the cover image. Simple DWT is added for the comparison purpose where it is not related to the specified work, however, it is related to similar works such as [24]-[25].

$$\text{PSNR} = 10log_{10}\frac{255^2}{\text{MSE}}\text{ (dB)} \tag{1}$$

The mean square error (MSE) is :

$$\text{MSE} = \left[\frac{1}{N\times N}\right]^2\sum_{i=1}^{N}\sum_{j=1}^{N}\left(X_{ij}-\bar{X}_{ij}\right)^2 \tag{2}$$

where:

N is the image size;

X_{ij} represents the original image pixels;

$\bar{X}_{ij}$ represents the stego-image pixels.

Table 3. The PSNR results.

Image	**Image Size**	**Gutub *et al.* [17]**	**Ghosal *et al.* [23]**	**Yazan *et al.* [21]**	**Simple DWT based Steganography**	**Proposed Algorithm**		
						BMP	**JPEG**	**TIFF**
Image 1	1024×1024 x3	57.73	56.29	57.94	74.1793	68.5244	68.0753	68.0791
Image 2	1024×1024 x3	58.10	56.68	58.20	73.9965	64.6591	68.4558	68.4558
Image 3	1024×1024 x3	57.90	57.02	57.93	74.0210	67.9923	67.6653	67.6653

It can be noted from Table 3 that the proposed scheme showed better results for all image types (BMP, JPEG and TIFF) when compared to the techniques in [17], [21] and [23], where it provides higher PSNR values with an average difference equal to 8 dB approximately, which makes the stego-image indistinguishable from the cover image, except the simple DWT-based steganography which gives higher PSNR values than the proposed technique. However, this does not mean that it is better, because the embedding procedure for the simple DWT is very easy, where the secret text can be obtained only by applying the DWT on the stego-image, then removing the 7left-most bits from each byte, where that threatens its security. The proposed scheme gives better security, because the steganography embedding procedure is difficult to be expected, in addition to that the indicator is not the same in the three high frequency bands (HL, LH and HH). Also, in case of the extraction of the embedded text, it becomes difficult to obtain the secret message due to high security added by the AES algorithm. As a result, AES encryption technique provides higher quality of the stego-image, but at the cost of higher complexity.

Table 4 shows the data load which can be embedded inside different loads of the images. It represents the maximum amount of secret data in bytes which can be embedded in each image.

Table 4. The payload results.

Image	**Image Size**	**Gutub et al,.. [17]**	**Ghosal's et al,.. [23]**	**Yazan et al,.. [21]**	**Simple DWT based Steganography**	**Proposed Algorithm**		
						BMP	**JPEG**	**TIFF**
		Hiding Capacity (Bits)	Hiding Capacity (Bits)	Hiding Capacity (Bits)	Hiding Capacity (Bits)	Hiding Capacity (Bits)	Hiding Capacity (Bits)	Hiding Capacity (Bits)
Image 1	1024×1024x3	1583486	1811022	1833746	2359272	485021	477122	477122
Image 2	1024×1024x3	1575400	1869612	2087466	2359272	700158	655622	655622
Image 3	1024×1024x3	1572370	1456352	1572900	2359272	649353	632528	632528

Table 4 presents the payload which is defined as "the maximum message size that can be embedded subject to certain constraints" [26]. The proposed algorithm has been tested using three different color image types (BMP, JPEG and TIFF). The hiding capacity is better in case of TIFF image than in BMP or JPEG. It is obvious that all the other works give higher payloads than the proposed algorithm. This is related to two reasons that are; using only three bands of the cover image (HL, LH and HH), which means that 25% of the image is not used for the embedding process, as well as using the PIT, where the indicator channel is not employed for hiding the secret message. However, high PSNR values can compensate this restriction -which will be explained later- where a trade-off between payload and PSNR is obtained, as shown in Figure 11, which resulted in high security with moderate capacity.

The degradation of quality of images can also be visually noticed by applying the histogram analysis that depends on the comparison between the cover image and the stego-image through the statistical tool histogram shown in Figures (8-10) which present the histogram comparison between the cover image and its corresponding stego-image, where the histograms are calculated for Red, Green and Blue channels separately. It can be shown that there are no visual changes between the original image histograms and the stego-image histograms that are detected, so that the proposed scheme becomes superior to other schemes in terms of high degree of security with moderate capacity.

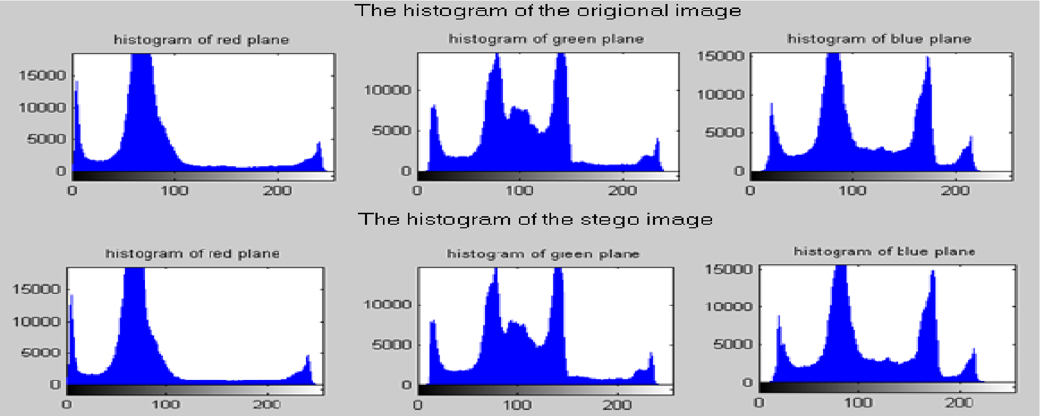

Figure 8. The histogram of the Red, Green and Blue channels of image 1. The upper part is for the original image and the bottom one is for the stego-image.

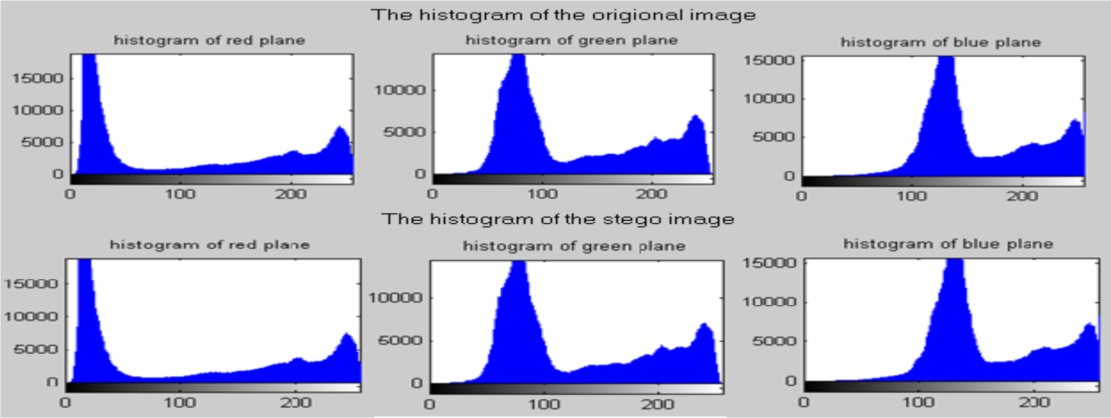

Figure 9. The histogram of the Red, Green and Blue channels of image 2. The upper part is for the original image and the bottom one is for the stego-image.

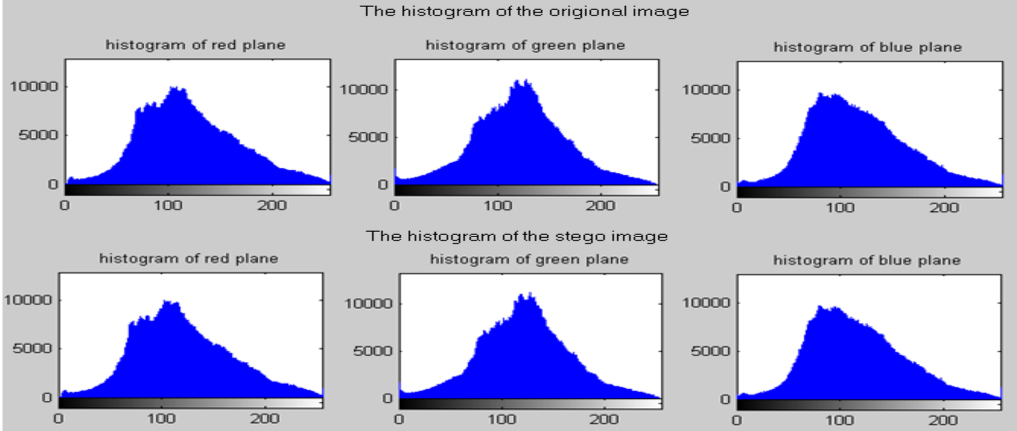

Figure 10. The histogram of the Red, Green and Blue channels of image 3. The upper part is for the original image and the bottom one is for the stego-image.

Table 5. The PSNR in dB for image 1, image2 and image 3 after the attacks.

Image after attack	Image Processing Operations		
	Addition of Gaussian noise	Radial blur	Median blur
Image 1	20.2184	24.5519	22.1014
Image 2	20.4400	20.1862	21.9934
Image 3	20.5697	27.2037	21.7112

The effects of increasing the payload on the PSNR and MSE for image 1, image 2 and image 3 are shown in Table 6 and represented in Figure 11 and Figure 12. The horizontal axis for Figure 11 shows the payload normalized to the value (2120 bytes) and the vertical axis shows the PSNR in dB. The curve shows that a degradation of the PSNR values is obtained as the payload increases, where the embedded text size is increased from 16960 bits to 200264 bits. For Figure 12, the horizontal axis shows the payload normalized to the value (2120 bytes) and the vertical axis shows the MSE.

It can be noticed that for image 1 in Table 3; algorithms in [17] and [21] give PSNR values which are approximately equal to 58 dB for an embedded text size of 2120 bytes. The proposed algorithm can embed approximately 5 times the value 2120 at the same PSNR (58 dB). Moreover, for the algorithm in [23], it gives a PSNR value equal to 56.29 dB when the embedded text message is 2120 bytes, which is approximately the same value obtained by the proposed algorithm, but when the size of the embedded text message is 9 times of 2120 bytes. This result shows the security of the proposed system, since it maintains high PSNR values albeit of increasing the payload to the maximum capacity, which means that the proposed algorithm is superior to other algorithms, where it maintains high security in spite of using the maximum capacity of the cover image. Such improvement in the proposed algorithm is due to employing the less significant bands in the DWT of the cover image.

Table 6. The effects of increasing the payload on the PSNR and MSE for image 1, image 2 and image 3.

Text Size (Bits)	**Image 1**		**Image 2**		**Image 3**	
	PSNR (dB)	**MSE**	**PSNR (dB)**	**MSE**	**PSNR (dB)**	**MSE**
16960	68.5244	0.0091	64.6591	0.0222	67.9923	0.0103
50288	62.8501	0.0337	59.3996	0.0747	63.2162	0.0310
83616	59.6919	0.0698	57.2645	0.1221	60.9395	0.0524
116944	57.2748	0.1218	55.4421	0.1857	59.4579	0.0737
150272	55.6721	0.1761	54.0982	0.2531	58.3095	0.0960
200264	53.9851	0.2598	52.8852	0.3346	56.7209	0.1384
266920	52.4574	0.3693	51.6802	0.4416	54.9500	0.2080

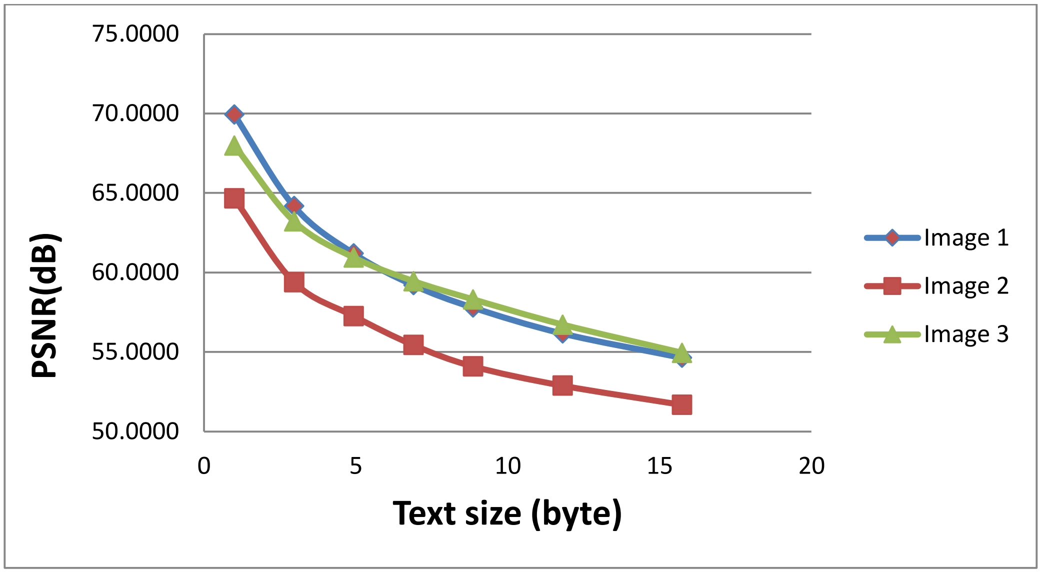

Figure 11. The effect of increasing the embedded text size on the PSNR of image 1, image 2 and image 3.

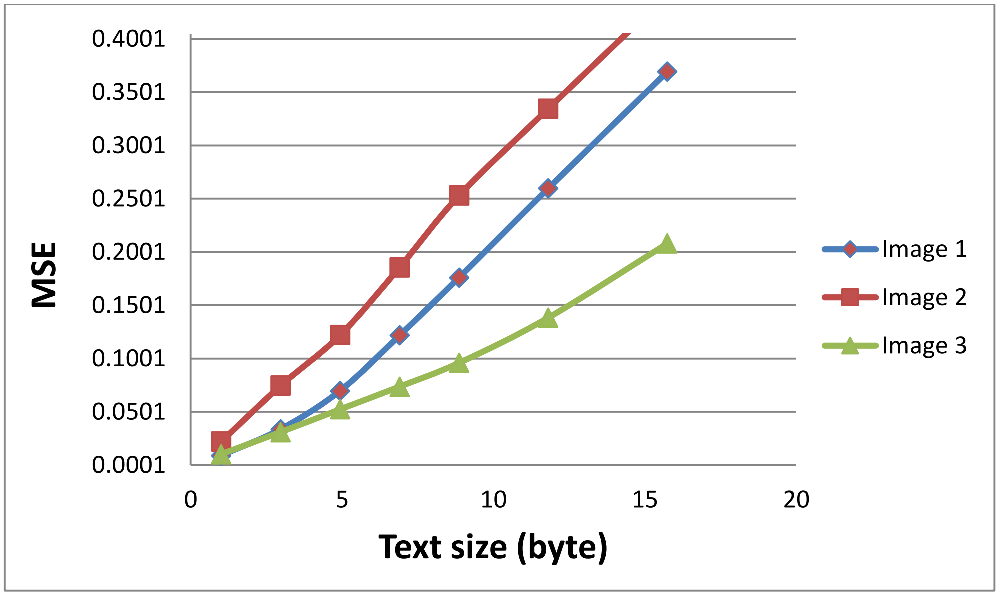

Figure 12. The effect of increasing the embedded text size on the MSE of image 1, image 2 and image 3.

4. CONCLUSION

In this paper, a combination between AES and DWT-based steganography with using PIT has been proposed. The stego-images are looking similar to the cover images and have high PSNR values. The histograms of the original images and stego-images have not shown visual changes. Therefore, an unauthorized observer will not be conscious of the existence of the hidden message. The payload that can be obtained by the proposed scheme is somewhat moderate with respect to other techniques. Moreover, the proposed scheme achieves higher PSNR, in addition to that the trade-off between payload and PSNR confirms the system security with good available capacity. Comparative analysis between the proposed technique and other existing ones has shown the superiority of the proposed technique from the perspective of providing high level of security with moderate capacity. Also, the robustness of the system is verified by applying some attacks. Future work would be directed towards building up special algorithms that improve both the security and capacity as well as increasing PSNR.

REFERENCES

[1] Gurpreet Kaur and Kamaljeet Kumar, "Digital Watermarking and other Data Hiding Techniques," International Journal of Innovation Technology and Exploring Engineering (IJJTEE), vol. 2, issue 5, 2013.

[2] Deepali V. Patil and Shatendra Dubey, "Review Paper on Image Steganography," International Journal of Research in Computer Applications and Robotics, vol. 2, issue 6, pp. 35-40, 2014.

[3] M. A. B. Younes and A. Jantan, "Image Encryption Using Block-based Transformation Algorithm," International Journal of Computer Science, vol. 35, issue 1, pp.15-23, 2008.

[4] Liu Tong and Qiu Zheng-Ding, "A DWT-based Color Image Steganography Scheme," Proceedings of IEEE 6th International Conference on Signal Processing, vol. 2, pp. 1568-1571, 2002.

[5] Anjali A. Shejul and U. L. Kulkarni, "A DWT-based Approach for Steganography Using Biometrics," Proceedings of IEEE 2010 International Conference on Data Storage and Data Engineering (DSDE), pp. 39-43, Feb. 2010.

[6] B. Raja Rao *et al.*, "A Novel Information Security Scheme Using Cryptic Steganography," Indian Journal of Computer Science and Engineering, vol. 1, no. 4, pp. 327-332, 2010.

[7] Lokesh Kumar, "Novel Security Scheme for Image Steganography Using Cryptography Technique," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, issue 4, April 2012.

[8] Falesh M. Shelke, Ashwini A. Dongre and Pravin D. Soni, "Comparison of Different Techniques for Steganography in Images," International Journal of Application or Innovation in Engineering and Management (IJAIEM), vol. 3, issue 2, 2014.

[9] Ahmed A. Abdelwahab and Lobha A. Hassan, "A Discrete Wavelet Transform Based Technique for Image Data Hiding," Proceedings of the 2nd National Radio Science Conference, pp. 1-9, Egypt, 2008.

[10] Vladimir Banoci, Gabriel Bugar and Dusan Levicky, "A Novel Method of Image Steganography in DWT Domain," Proceedings of IEEE 21st International Conference on Radioelektronika, pp. 1-4, April 2011.

[11] J. K. Mandal and M. Sengupta, "Authentication Secret Message Transformation through Wavelet Transform-based Sub-band image Coding (WTSIC)," Proceeding of IEEE 2010 International Symposium on Electronic System Design (ISED), pp. 225-229, Dec. 2010.

[12] Souvik Roy and P. Venkateswaran, "Online Payment System Using Steganography and Visual Cryptography," 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1-5, Mar. 2014.

[13] Pye Pye Aung and Tun Min Naing, "Implementation of Cryptography and Image Steganography with New Security Feature," International Conference on Advances in Engineering and Technology (ICAET'2014), 2014.

[14] F. M. Septimin, Mircea Valdutin and P. Lucian, "Secret Data Communication System using Steganography, AES and RSA," 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), pp. 339-344, Oct. 2011.

[15] Kamal and Lovnish Bansal, "Enhancement Key of Cryptography and Steganography Using RSA and Neural Network," International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 3, issue 5, 2014.

[16] S. K. Muttoo and Sushil Kumar, "A Multilayered Secure, Robust and High-Capacity Image Steganographic Algorithm," World of Computer Science and Information Technology Journal (WCSIT), vol. 1, no. 6, pp. 239-246, 2011.

[17] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen and Aleem Alvi, "Pixel Indicator High-Capacity Technique for RGB Image based Steganography," IEEE International Workshop on Signal Processing and Its Applications, University of Sharjah, Sharjah, U.A.E., 2008.

[18] Ruchi R. Vairagade, Shubhangini Ugale and Prachi Pendke, "Review on 128-Bit Advanced Encryption Standard Algorithm with Fault Detection," International Journal of Advanced Information and Communication Technology (IJAICT), vol. 1, issue 7, 2014.

[19] Mohammad Abdullatif, Othman O. Khalifa, R. F. Olanrewaju and Akram M. Zeki, "Robust Image Watermarking Scheme by Discret Wavelet Transform," Proceedings of IEEE 5th International Conference on Computer and Communication Engineering (ICCCE), pp. 316-319, Sept. 2014.

[20] Swapnali Zagade and Smita Bhosale, "Secret Data Hiding in Images by Using DWT Techniques," International Journal of Engineering and Advanced Technology (IJEAT), vol. 3, issue 5, 2014.

[21] Yazan Abdallah and H. Seidan, Enhancement of a Steganographic Algorithm for Hiding Text Messages in Images, M. Sc. Thesis, Middle East University, 2013.

[22] Saleh Saraireh, "A Secure Data Communication System Using Cryptography and Steganography," International Journal of Computer Networks and Communications (IJCNC), vol. 5, no. 3, 2013.

[23] S. K. Ghosal, "A New Pairwise Bit-based Data Hiding Approach on 24-Bit Color Image Using Steganographic Technique," Greater Kolkata College of Engineering & Management, Kolkata, India, 2011.

[24] T. Vanitha, Anjalin D'Souza, B. Rashmi and Sweeta D'Souza, "A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, special issue 5, 2014.

[25] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security (IJCSS), vol. 4, issue 6, 2011.

[26] R. Chandramouli and N. D. Memon, "Steganography Capacity: A Steganalysis Perspective," Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003.

ملخص البحث:

تستخدم تقنيات الإخفاء من أجل نقل البيانات بأمان، إلا أنّ الرسائل الناتجة غير القابلة للقراءة عادة ما تجذب انتباه الآخرين، ولهذا يتم إخفاء المعلومات السرية على نحوٍ لا يمكن معه للمقتحمين أن يكتشفوا وجود البيانات السرّية.

تقترح هذه الورقة تقنية محسّنة تجمع بين خوارزمية معيار الإخفاء المتقدم (AES) والاختزال، وتستفيد من مزايا استخدام معامِلات الترددات العالية لصورة التغطية عن طريق تطبيق التحويل المجرّد للمويجات (DWT). وقد تم تطبيق التقنية المقترحة لدراسة أثر إخفاء الرسالة السرّية المخفية في صورة الأحمر والأخضر والأزرق المؤلفة من 24 بِت (bit). وتم تقييم أداء الطريقة المقترحة من حيث: المعدل الأقصى للإشارة إلى الضجيج (PSNR)، وسعة إخفاء الحمل الصافي، وتحليل توزيع الرسم البياني النسيجي.

من ناحية أخرى، تقدم هذه الورقة مقارنة بين التقنية المقترحة وأربعة من الأعمال السابقة الأخرى ذات العلاقة بموضوع الدراسة. وقد كشفت النتائج التجريبية أنّ الطريقة المقترحة في هذا البحث تعطي درجة عالية من الأمان في إخفاء البيانات، إضافة إلى أنها تبدي حصانة ضدّ الهجمات ومحاولات الاختراق المختلفة.