© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

Text Hiding in Coded Image Based on Quantization Level Modification and Chaotic Function

Shams N. Abd-Alwahab[1*], Mousa K. Wali[2], Mehdi F. Bonneya[3]

[1]Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad, IRAQ

[2]Department of Electronic Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad, IRAQ

[3]Department of Electrical Technical, Kut Technical Institute, Middle Technical University, Baghdad, IRAQ

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2021.13.01.013
Received 3 March 2019; Accepted 30 November 2019; Available online 30 January 2021

Abstract: Information hiding deals with hiding the consequences of secret information into the cover medium with minimum distortion as possible. In this paper, a method of hiding text in the coded image is presented which is based on quantization level modification. There is important data needed to be send from source to destination with security. The used image is transformed into the wavelet domain by using the Discrete Wavelet Transform (DWT) and the coefficients of transform are partitioned into predefined blocks sizes. Specific threshold has been used to classify these blocks into two types named smooth and complex. Each type has its own method of text hiding (binary data), for smooth blocks, secret bits which represent the text data are switched by the bitmap. In order to reduce distortion, the quantization levels are modified. To reach extra embedding payload, the quantization level could carry extra two bits depending on another threshold. The complex block carries one data bit on each block and quantization levels are swapped to reduce distortion with bitmap flipping. The results of the proposed method show high signal to noise ratios, also, studying capacity is an important concept in this work.

Keywords: Discrete wavelet transform, text hiding, henon map

1. Introduction

The key objective of image steganography is to hide the secret data into different embedding medium called as carriers. These carriers can be images, video, or audio files. In this paper, recent stenographic techniques for image files are used. Imperceptibility, embedding capacity, and robustness are the key issues of image steganography [1-3]. Most of these recent techniques are work on analyzing the key issues of steganography and discussing the merits and demerits, to identify the suitability for data hiding method which will provide guidance to the people working in this field. Image data hiding can be executed in the spatial and compressed domain. Data hiding technique in spatial domain, directly modifying the pixel values of the cover image in the spatial domain for embedding data [4-6]. Since images have richer redundancy in the spatial domain than those in the complex domain, therefore, a data hiding technique offers considerably higher payload and image quality in the spatial domain. On the other hand, after image compression, the data redundancy decreases, therefore, the embedding capacity and quality of a compressed data hiding technique tends to be lower. The simple and efficient image compression technique among these lossy techniques is a Block Truncation Coding (BTC).

Two quantization levels (a_i, b_i) and a bitmap B_i is applied through compressed code of an image block $C_i$by using an Absolute moment block truncation coding (AMBTC). AMBTC has attracted attention to investigate data hiding because it requires insignificant computation cost and provides very acceptable image quality, therefore, the AMBTC is

*Corresponding Author: shamsnaseer3a@gmail.com

a compressed image [7]. This work presents an approach different from other works in hiding in the high-frequency bands of wavelet domain and keep the low frequency without modifying. From another side, the embedding information has a specific mapping and all coded data will scramble.

2. Literature Review

There are many previous types of research related to this work:

S. Uma Maheswari, D. Jude Hemanth, 2015 [8] enhanced the performance of image hiding system using transformation and optimization techniques such as genetic algorithm (GA) and partial swarm optimization (PSO) for selecting the best coefficients to embed secret data.

Wien Hong, Tung Shou Chen, Zhaoxia Yin, Bin Luo, Yuanbo Ma, 2016 [7] rely on quantization level modification and perturbation technique. This method depends on partition an image into blocks that classified as smooth and complex, i.e.: two methods of embedding secret data for each block type.

R. Ranjith Kumar, S. Jayasudha, S. Pradeep, 2016 [9] presented a technique for hiding data in an intermediate significant bit (ISB) and a least significant bit (LSB) of the cover image. Chaotic maps used for mapping of data hiding and for permutation order for cover image encryption.

Wien Hong, 2018 [10] emphasis data hiding using (AMBTC) by partitioning an image into blocks, each block represents by the trio: two quantization levels and an asymmetrically distributed bitmap. The proposal hides high payload with significant image quality.

Nabanita Mukherjee (Ganguly), Goutam Paul, Sanjoy Kumar Saha, 2018 [11] proposed steganography in spatial domain using pixel value differencing (PVD) or sample value differencing (SVD) and Galois field (GF) by provide two security layers for hiding secret message. The proposal embeds (2 to 6 bits for each pixel) in an image and (6 to 13 bits per sample) in audio.

3. Methodology

A method for text hiding in the image is presented in this paper that use steganography techniques to provide more security. This method used the coding technique and three kinds of hiding methods depend on the smoothing of the pixel in each block. In this work, the used cover media is image, this image is transformed in to DWT to split the important high-value approximation coefficients for hiding the information from other unimportant low values details. Another issue is to build a map. The total encoded cover image is scrambled using the key generation. The proposed method consists of two phases forward and backward phases, as the hiding method represent the forward phase that needs input image as covered image and secret text as secret information. The input image split into three color bands red, green, and blue (RGB) and pass through sequences of stages to produce the stego-image, as explain in Figure 1.

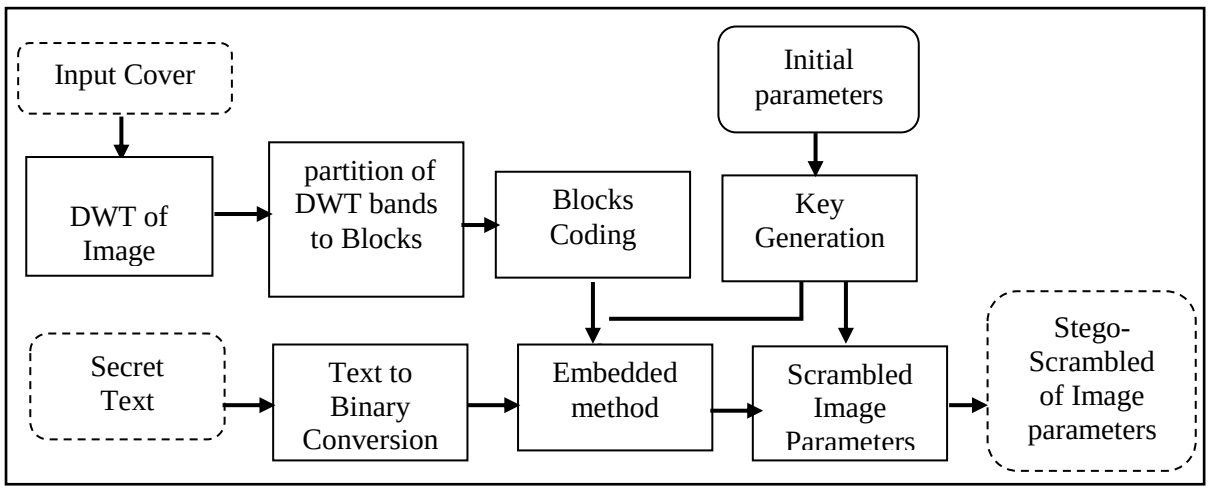


Fig. 1 - Block diagram of proposed hiding method

3.1 Hiding Method

The first method is Quantization Level Modification technique (QM) embedded 16 bits for each (4×4) block for example; By replacing each secret bit with bitmap block of the image. The bitmap obtained by find threshold of each block by finding the mean of pixels' intensity (any pixel greater than mean represent by one otherwise is zero), additionally, find two mean values of block pixels one is greater than or equal to threshold called b_i, and other is lower

than threshold called a_i. The second method used Quantization Perturbation technique (QP) that compare between two specified thresholds (T_m, T_s) if the condition was true then the QP technique is performed to embed two bits secret data into quantization levels Finally, the third method was lossless embedding technique by swap the values of $a_i$with b_i and flipping B_i (bitmap) that represent the block, if the embedded bit was one otherwise keep the values without change. QM is applied when the condition $|a_i - b_i| \leq T_m$ is true, QP is applied when $T_m \geq T_s$, lossless is applied when the condition $|a_i - b_i| > T_m$ is true.

3.2 Discrete Wavelet Transform

Whether the stationary or non-stationary signal, it can be analyzed by the wavelet transform (WT). Where the WT has an extensive application in the analysis of signals to be decomposed into a set of fundamental signals. In addition, the signal will be represented by sine and cosine functions of unlimited length like the Fourier transform (FT). The obtained frequency spectrum from the FT is simple to separate the frequency contents of the analyzed signal, but it is impossible to deduce the happening time for the frequency spectrum of the signal components. While the WT gives information on the evolution of the frequency contents of a signal over time. As mentioned before, the WT decomposed the signal into many scales demonstrating diverse frequency bands, besides, at each scale, the position of the WT can determine the important time characteristic where the electrical noise can be recognized and efficiently removed. Since electrical noise is more likely to exhibit high-frequency fluctuations, therefore, important information can be extracted from high-frequency components by using short-time wavelets. Long-term wavelets allow to extracting information from low frequencies [12,13]. In this research, each band of the color image is used as a grayscale image and could be used for hiding information. The image transforms into one level by Haar discrete wavelet transform as shown in Figure 2 to produce four bands; Low-Low (LL), High-Low (HL), Low-High (LH), and High-High (HH) bands. The Low-Low band consists of significant value of image information. Therefore, embedding may be used in any of other bands.

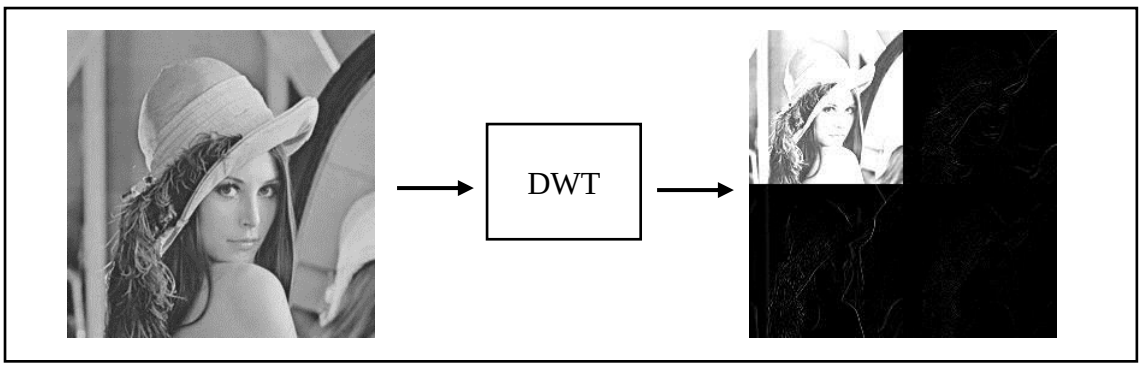


Fig. 2 - Image discrete wavelet transform

3.3 Chaotic Function and Henon Map

Chaotic map (evolution function) demonstrates a sort of chaotic behavior in mathematics. It can be used for discrete-time or a continuous-time depending on its type. Maps may be parameterized by the parameter. Discrete maps usually take the method of repeated functions. Chaotic maps commonly used in the study of dynamical systems [8,14]. Frequently, chaotic maps generate fractals. Though the fractal may be constructed by a repeated process, some fractals are studied as sets rather than in terms of maps that generate them [15], since there are many diverse iterative ways to generate the same fractal.

The Henon Map was introduced by Michel Henon as a simplified model of the Poincare section of the Lorenz model. For the classical map, an initial point of the plane will either approach of a set of points known as the Henon strange attractor, or diverge to infinity. The Henon attractor is a fractal, smooth in one direction and a Cantor set in another. Numerical estimates yield a correlation dimension of 1.25 ± 0.02 [16] and a Hausdorff dimension of 1.261 ± 0.003[17] for the attractor of the classical map. Chaotic values can be generated from applying equations (1 & 2) which is iterated *n* times to generate the required elements.

$$x(n+1) = 1 - a \times x(n)^2 + y(n) \quad (1)$$

$$y(n+1) = b \times x(n) \quad (2)$$

The constant values 'a=1.76' and 'b=0.1' were used to get a random sequence [18].

The Henon Map is used for the key generation with an initial value that generates real numbers in period (0, 1). These numbers will be used in two directions: The first direction is to map the hiding information and the second direction is to substitute the output-codded values of forwards method as shown in Table 1. The blocks that represent by (m × m) are used for embedding, and for each block denoted by C_i , compute the average pixel value in C_i denoted by $\overline{C_i}$. The

bitmap B_i can be constructed and the lower quantization level a_i is gotten by rounding the mean value of the pixel in C_i with values less than the value of C_i , similarly with b_i. To decode the AMBTC trio (a_i,b_i,B_i), zero's values in B_i are decoded by a_i ,and one's values in B_i are decoded by b_i ,consequently, decode the image $\widetilde{C_i}$.

Table 1 - An example of chaotic selected blocks based on henon map

Index	Block #	Index	Block #	Index	Block #
1	12	7	137	13	329
2	4	8	169	14	361
3	99	9	201	15	393
4	6	10	233	16	425
5	73	11	265	17	457
6	105	12	297	18	489

The process of creating secret text is done by firstly converting the input text to ASCII code at first. The second step is converting it to binary form. This binary sequence will be embedded in the covered band in non-uniform length depend on a specific threshold as explained in the embedding stage [13,18]. Embedding procedure of the proposed method is explained in the flowchart of the Figure 3. The steps of embedding method are as follow:

Step 1: Specify (T_m) as the smallest threshold, therefore, all the secret data S can be embedded.
Step 2: Use the QM technique and embed the data by replacing the bitmap Bi with secret data S_i and modify the corresponding quantization levels (a_i,b_i) to($\widehat{a_i}$, $\widehat{b_i}$) such that the distortion between the original and stego AMBTC blocks is minimal.

- Scan each trio in $\{a_i, b_i, B_i\} i^N = 1$, and calculate $d_i = |a_i - b_i|$, if $d_i \leq T_m$, then QM technique is employed to embed m × m secret bits, and to calculate the best quantization levels ($\widehat{a_i}$; $\widehat{b_i}$) that minimize the distortion.
- Let B_i=$\{\beta_{i,j}\}_{j=1}^{m\times m}$ be the bitmap of ($i-th$) block, and S_i=$\{s_{i,j}\}_{j=1}^{m\times m}$ be the secret data to be embedded. Since the embedding is performed by replacing B_i with S_i, the distortion occurs at $S_{i,j} \neq \beta_{i,j}$.
- If $T_m \geq T_s$, then the QP technique is performed to embed two bits secret data into quantization levels, (providing that the conditions mod ($\hat{a}i$, 2) =s_1, mod ($\hat{b}i$, 2) =s_2 and $|\hat{a}i - \hat{b}i| \leq$T are met).

Step 3: If $d_i \leq T_m$ and $T_m < T_s$,, then QM embedding technique is performed only to embed m × m bits into the bitmap of the scanned trio.
Step 4: If d_i > Tm, lossless embedding technique is done to embed one bit by swapping the quantization levels together with bitmap flipping, (That is, if the embedded bit is equal to '0', the stego AMBTC trio is recorded by (a_i,b_i, B_i). If the embedded bit is '1', the AMBTC trio is recorded by (b_i, a_i,$\overline{B_i}$). Since the decoded image block using the trio (a_i,b_i, B_i) is identical to that of (b_i, a_i,$\overline{B_i}$) , this operation provides no distortion result but embeds one additional bit).
Step 5: The $\{a_i^S, b_i^S, B_i^S\}_{i=1}^N$ refers to the embedded trio. Keep repeating steps 2–4 until all the secret data are embedded.

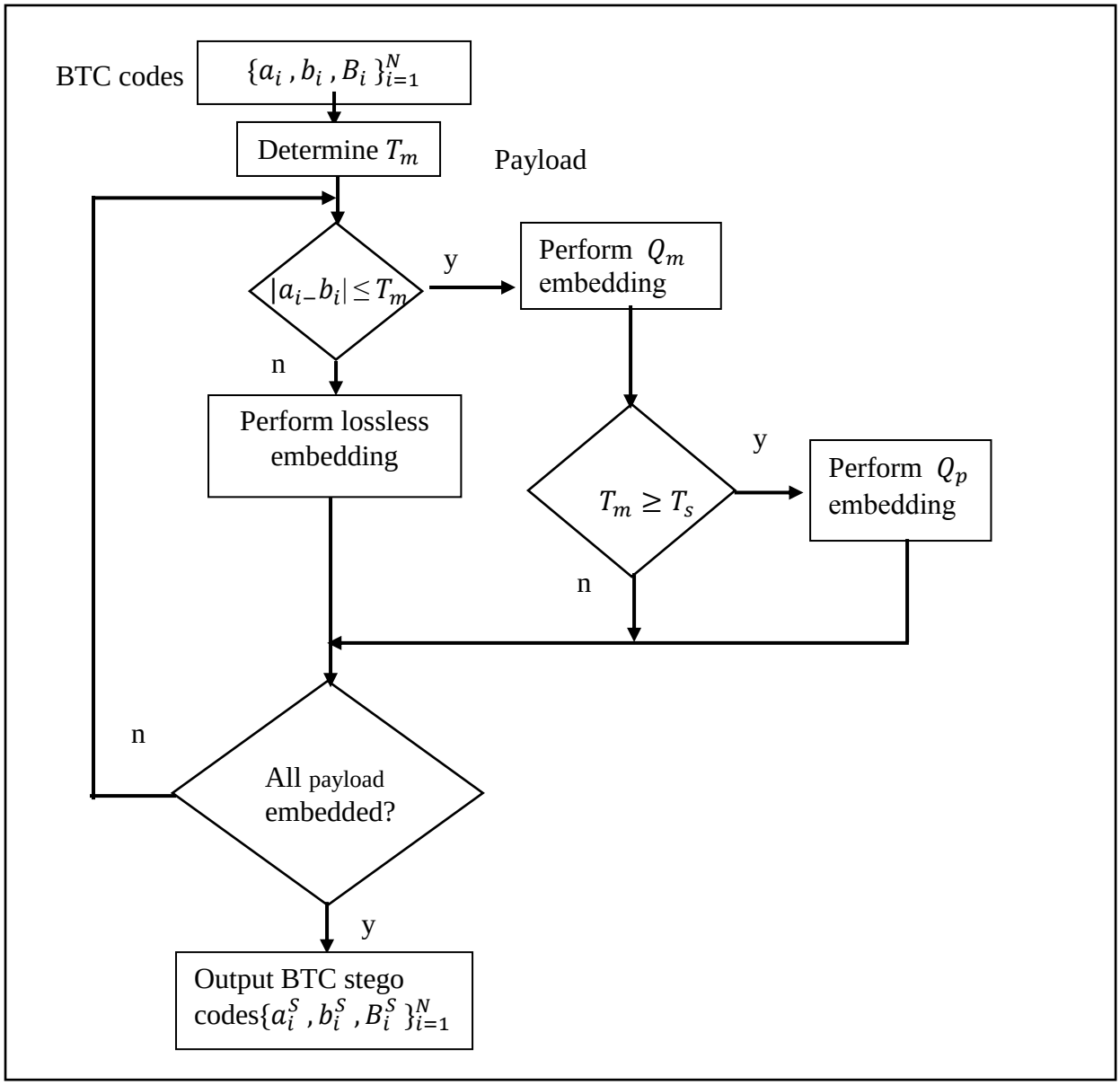


Fig. 3 - Embedding flowchart of the proposed method

3.4 Proposed Extraction Method

The extraction method is backward phase of the proposed method that uses some similar stages of forward in reverse order. The total steps of extraction method are illustrated in Figure 4.

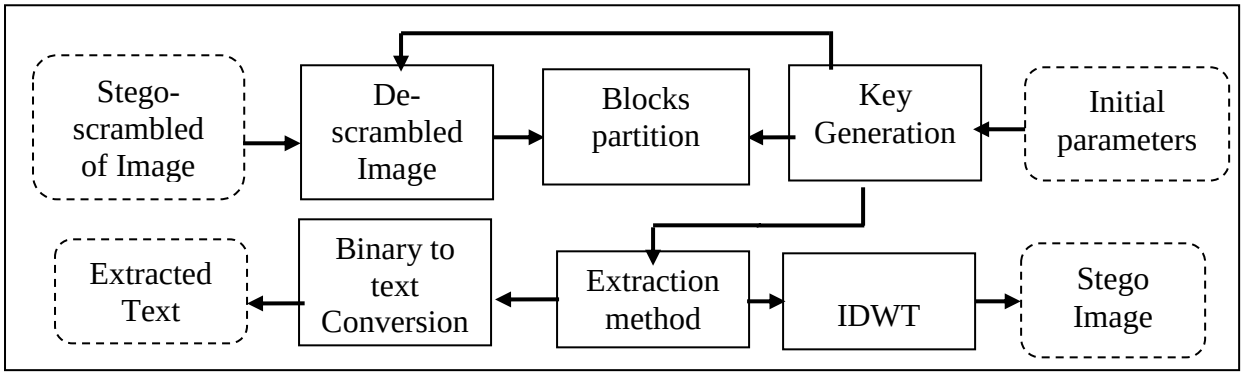


Fig. 4 - Block diagram of the proposed extraction method

Henon map is also used to generate the real number and multiplied by power ten decimal number. As well as, the result will round and modules to number N that specified in the transmitter side [4,5]. In addition, the same key generated by Henon map in scrambling order can be used in the three color bands of the image [14, 15]. Inverse DWT will be used to get the original image with minimal distortion. The extracted data are in binary form and these binary secret data will be converted to ASCII code to be finally converted to character. The Extraction procedure method used to extract the original text is as follows:

Step 1: Scan each stego trio in $\{a_i^S , b_i^S , B_i^S \}_{i=1}^N$.

Step 2: Compute $d_i = |ai^S - bi^S|$.

Step 3: If di ≤ Tm, from Bi^S all m^2 bits are extracted. Two additional bits are extracted from the LSBs of ai^S and bi^S if $T_m \geq T_s$ is satisfied,

Otherwise

If ai^S<bi^S, a bit '0' is extracted otherwise a bit '1' is extracted.

Step 4: by repeating steps 2–3 besides concatenating all the extracted data bits; the embedded secret data can be extracted.

3.5 Coding Example

Here a simple example to explain the AMBTC and DWT embedding, scrambling and extraction technique as shown in Figure 5:

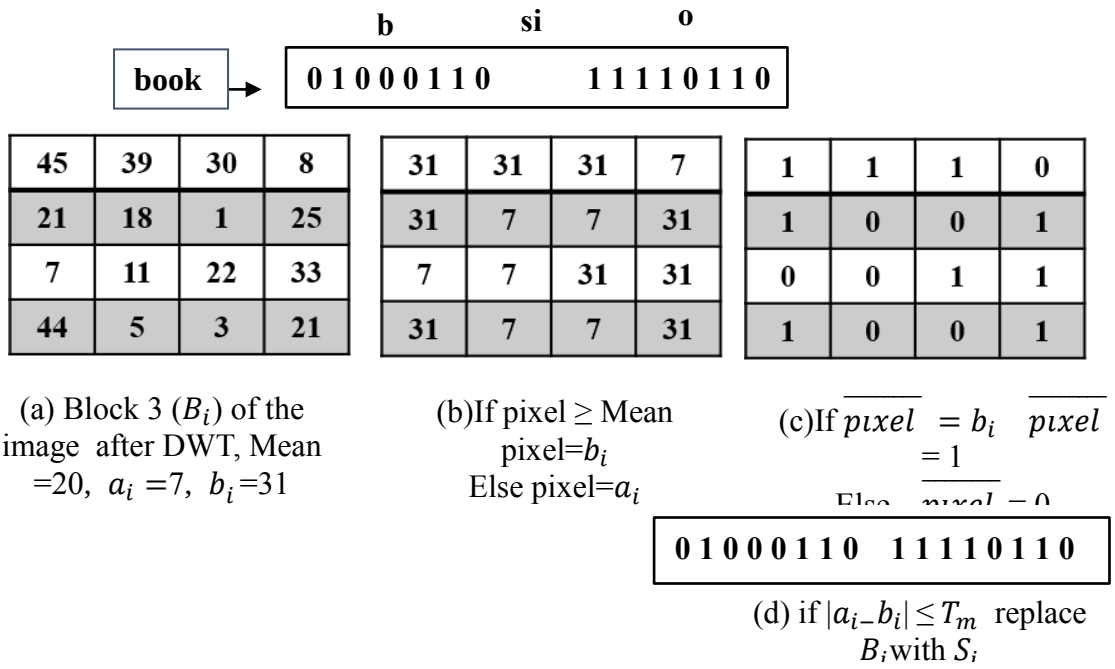


Fig. 5 - An example of AMBTC coding

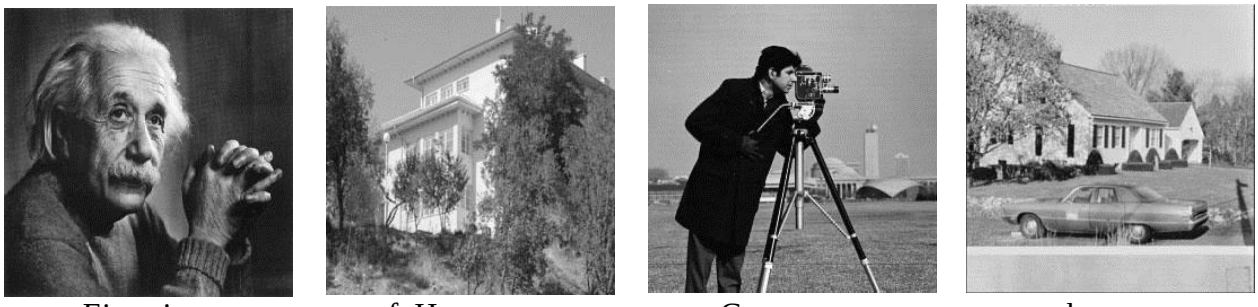
4. Experimental Result

The proposed method is applied on the selected images to test grayscale images of size 256×256, including Lena, Peppers, Elaine, Baboon, Einstein, House, Cameraman, and car, as shown in Figure 6. A block of size 4×4 is used and the secret data is a text converted to binary form with variable length. The stego images: Lena, Peppers, Elaine, Baboon, Einstein, House, Cameraman, and car are shown in Figure 7.

a. Lena b. Peppers c. Elian d. Baboon

e. Einstein f. House g. Cameraman h. car

Fig. 6 - Tested images



e. Einstein f. House g. Cameraman h. car

Fig. 7 - Stego-images

The proposed method is tested and evaluated by finding the Mean Square error (MSE) of the stego-image with respect to original image and the results are shown in Table 2 and in Figure 8. The experiments result explains that the MSE of the original and stego image both are very closed and the average of hiding in 30, 60, 90 and 120 bytes are (8.37803), (8.65916), (8.76351) and (8.8444) respectively.

Table 2 - MSE of tested images

Image #	30 bytes	60 bytes	90 bytes	120 bytes
Lena	5.16595	5.49307	5.73611	5.73706
Peppers	2.86090	2.86157	2.87018	2.87866
Elian	3.35324	3.36429	3.38309	3.47316
Baboon	20.31096	21.97586	21.99210	22.03650
Einstein	5.89449	5.93538	6.13173	6.13466
House	8.15610	8.35890	8.43039	8.51923
Cameraman	14.78104	14.78131	14.98616	14.99052
Car	6.50163	6.50291	6.57838	6.98541

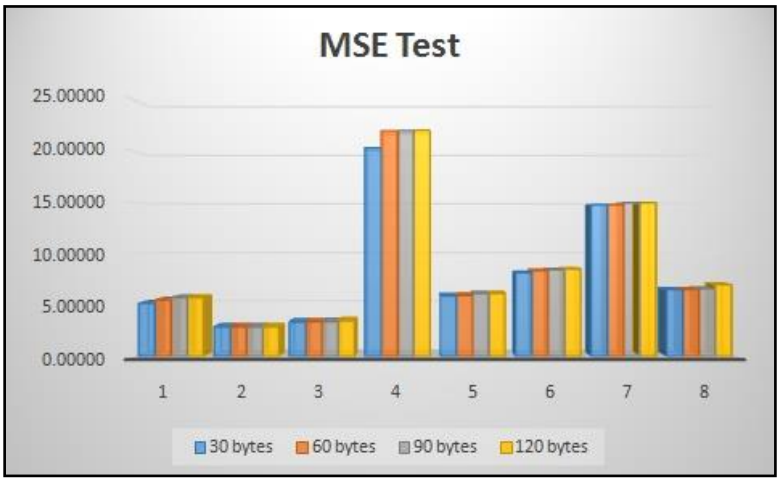


Fig. 8 - MSE of Tested images

The previous Figure 8 explain all MSE values for all tested images when embedding different size of data and all result show low values that mean the proposal didn't make distortion in cover image at all.

The second measure is the peak signal to noise ratio (PSNR). The PSNR values are explained in Table 3 and Figure 9. The obtained PSNR values of the original and stego image are almost the same, and the average of hiding in 30, 60, 90 and 120 bytes are (38.67142),(39.70120),(39.63662) and (39.58087) respectively.

Table 3 - PSNR values of the tested images.

Image #	30 bytes	60 bytes	90 bytes	120 bytes
Lena	40.99930	40.73265	40.54463	40.54391
Peppers	43.56578	43.56476	43.55171	43.53890
Elian	42.87616	42.86187	42.83767	42.72356
Baboon	35.05350	34.71134	34.70814	34.69938
Einstein	40.42634	40.39632	40.25497	40.25290
House	39.01598	38.90931	38.87233	38.82680
Cameraman	36.43375	36.43367	36.37390	36.37264
Car	40.00058	39.99972	39.94961	39.68888

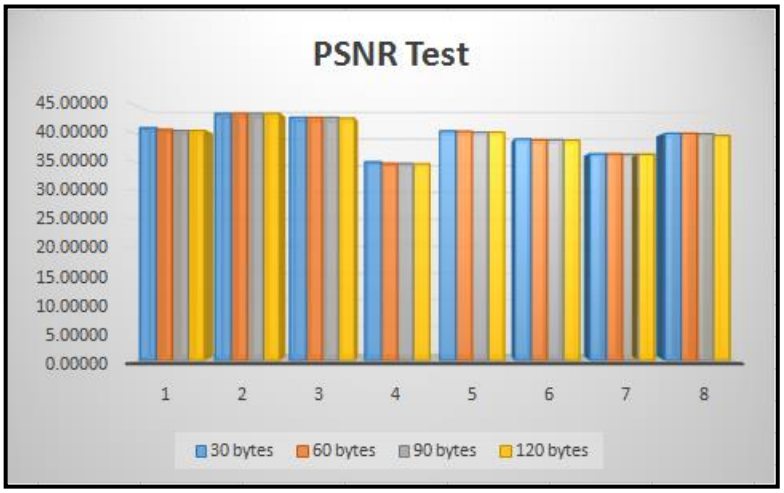


Fig. 9 - PSNR values of the tested Images

The objective measurement (PSNR) of image quality used for testing all images and the result have accurate values between 35%-40% as explain in Figure 9 that is accepted values which denotes that no distortion in cover image. this test always used in steganography to compare stego-image with original image.

The third measure is the structural similarity index (SSIM), and the obtained SSIM values are explained in Table 4 and Figure 10. The SSIM values of hiding in 30, 60, 90 and 120 bytes are (0.99023), (0.98993), (0.98981) and (0.98970) respectively.

Table 4 - SSIM values of the tested images

Image #	30 bytes	60 bytes	90 bytes	120 bytes
Lena	0.99429	0.99392	0.99374	0.99374
Peppers	0.99659	0.99659	0.99658	0.99656
Elian	0.99178	0.99174	0.99169	0.99146
Baboon	0.98007	0.97851	0.97843	0.97832
Einstein	0.98940	0.98927	0.98899	0.98896
House	0.98952	0.98927	0.98913	0.98897
Cameraman	0.98654	0.98654	0.98638	0.98636
Car	0.99367	0.99366	0.99360	0.99328

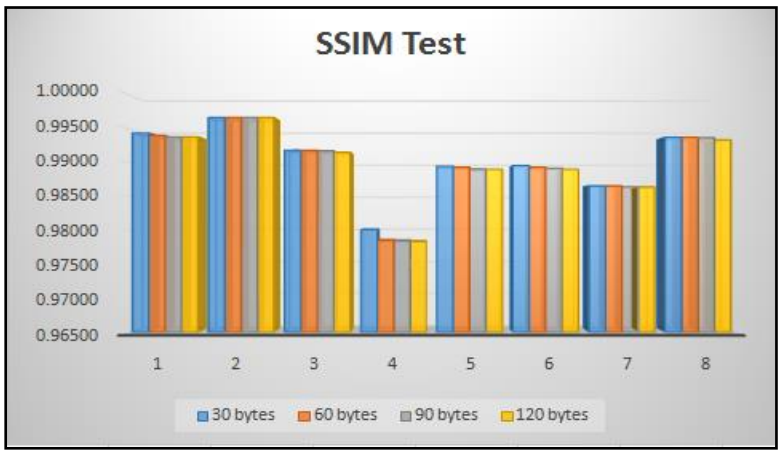


Fig. 10 - SSIM values of the tested Images

The other objective quality test (SSIM) explain in Figure 10 which all values of tested images approximated to 1.0. this objective test considers 1.0 as optimized value and when its value approximate to it means accurate quality. Table 5 explains a comparison between this work and other recently existing works.

Table 5 - A comparison between this work and other recently existing works

References	Methodologies	Results
Wien Hong [10].	Data Hiding Based on Block Truncation Coding Using Pixel Pair Matching Technique.	PSNR is 32.274 dB.
R. Ranjith, S. Jayasudha and S.Pradeep [9].	Secure data hiding in encrypted images by using tent map and logistic map.	PSNR is 44 dB.
Wien Hong, Tung Shou Chen, Zhaoxia Yin, Bin Luo and Yuanbo Ma [7].	(AMBTC) using quantization level modification and perturbation technique.	PSNR is 32.82625 dB.
Nabanita Mukherjee, Goutam Paul and Sanjoy Kumar Saha [11].	Pixel value differencing (PVD) and Sample value differencing (SVD).	PSNR is 37.9625 dB.
S. Uma Maheswari and D. Jude Hemanth [8].	Contourlet and fresnelet transforms and for optimization using Genetic Algorithm (GA) and Partical Swarm Optimization (PSO).	PSNR are 46.93 dB for Contourlet with GA, 50.64 dB for Contourlet with PSO,52.38 for fresnelet with GA and 52.56 dB fresnelet with PSO.
Proposed Method	Text Hiding in Coded Image Based on Quantization Level Modification, Chaotic Function and DWT	PSNR in 30, 60, 90 and 120 bytes are (38.67142),(39.70120),(39.63662) and (39.58087) respectively.

the comparison in previous Table 5 explain that the proposed method has best values in PSNR with respect to other values of related work. The efficiency of proposal denotes a less distortion in cover image (tested image). The proposed technique achieved 39.58087 PSNR in hiding 120 bytes using DWT, and this result give more security without the need to use any intelligent algorithm which may take extra time.

5. Conclusion

AMBTC data hiding based DWT method is used to hide text data into the coded image. The mapping of data hiding is specified using Henon map. Two quantization levels are re-calculated when embedding data in smooth blocks, to minimize image distortion with ease of implementation and low computation complexity. Moreover, the adjustable diverse threshold values can be employed unlike other applications based on appropriateness and demand. It is noticeable that the proposed method is a fragile data hiding method because any modification to the cover object distorts the embedded data. Therefore, the proposed method can be used in applications where fragile characteristics are demanded such as image authentication or tampering detection. The proposed method improves both embedding capacity and the imperceptibility in the experiment results. DWT increases the embedding capacity and keeping the MSE and PSNR ratios quite as possible. Using mapping for hiding location increases the secrecy of sending information and increases the complexity of information extraction by unauthorized people. Thus, the experimental results demonstrate that the proposed method is effective and it provides better visual quality for stego images in comparison to other previous works.

References

[1] Manjunath Prasad and K. L. Sudha (2011). Chaos Image Encryption using Pixel shuffling. Computer Science & Information Technology (CS & IT)

[2] Fatemeh Ranjbar, Yahya Forghani, Davoud Bahrepour (2018). High performance 8-bit approximate multiplier using novel 4:2 approximate compressors for fast image processing. International Journal of Integrated Engineering, 10

[3] M. Nishat Akhtar, Junita Mohamad Saleh, C. Grelck (2018). Parallel Processing of Image Segmentation Data Using HadoopInternational. Journal of Integrated Engineering, 10

[4] H.B.Kekre, Tanuja Sarode, Pallavi N. Halarnkar and Debkanya Mazumder (2014). Comparative Performance of Image Scrambling in Transform Domain using Sinusoidal Transforms. International Journal of Image Processing (IJIP) , 8

[5] Dong Wang, Chin-Chen Chang, Yining Liu, Guoxiang Song and Yunbo Liu (2015). Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values. International Journal of Network Security, 17

[6] Oussama Kadri , and Zine-Eddine Baarir (2016). Still Image Compression Using Curvelets and Logarithmic Scalar Quantization Technique. IEEE

[7] Wien Hong, Tung Shou Chen, Zhaoxia Yin, Bin Luo and Yuanbo Ma (2016). Data hiding in AMBTC images using quantization level modification and perturbation technique. Springer

[8] S. Uma Maheswari and D. Jude Hemanth (2015). Performance enhanced image steganography systems using transforms and optimization techniques. Springer

[9] R. Ranjith, S. Jayasudha and S. Pradeep (2016). Efficient and secure data hiding in encrypted images: A new approach using chaos. Information Security Journal, 25

[10] Wien Hong (2018). Efficient Data Hiding Based on Block Truncation Coding Using Pixel Pair Matching Technique. Symmetry, vol.36

[11] Nabanita Mukherjee, Goutam Paul and Sanjoy Kumar Saha (2018). An efficient multi-bit steganography algorithm in spatial domain with two-layer security. Springer

[12] Said E. El-Khamy, Noha O. Korany and Marwa H. El-Sherif (2016). A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. Springer

[13] Deepesh Rawat and Vijaya Bhandar (2013). Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method. International Journal of Computer Applications , 67

[14] Guodong Ye (2009). Image scrambling encryption algorithm of pixel bit based on chaos map. ELSEVIER

[15] Fan Jing and Huang Fei (2009). FAN Transform in Image Scrambling Encryption Application. IEEE

[16] Amit Phadikar and Santi P. Maity (2011). Data hiding based quality access control of digital images using adaptive QIM and lifting. ELSEVIER

[17] Malini Mohan & Anurenjan P.R (2011). A New Algorithm for Data Hiding in Images using Contourlet Transform. IEEE

[18] Younho Lee, Heeyoul Kim, Yongsu Park (2009). A new data hiding scheme for binary image authentication with small image distortion. ELSEVIER