APPLICATIONS OF
MODELLING AND SIMULATION
http://arqiipubl.com/ams eISSN 2600-8084 VOL 6, 2022, 20-27

Development of a Non-Separable Integer-to-Integer Wavelet Transform-Based Digital Image Steganography System

M. A. Idakwo*, M. B. Mu'azu, E. A. Adedokun and B. O. Sadiq

Department of Computer Engineering, Ahmadu Bello University Zaria, Nigeria

*Corresponding author: mondabutu@gmail.com

Submitted 23 September 2021, Revised 24 October 2021, Accepted 02 November 2021, Available online 27 January 2022.

Abstract: This paper develops a high payload and imperceptible digital image steganography system using a non-separable integer wavelet transform and diamond encoding. This became necessary to effectively utilize all the redundant bits in an image without any distortion. The developed non-separable integer-to-integer transform is responsible for decomposing the digital image into the frequency domain and has an advantage of resiliency to attacks, 75% lower rounding operations, and 50% lifting steps when compared with existing integer wavelet transform. The Haar was adopted as analyzing and synthesizing filter owing to its higher visual quality of 68.73 dB, 0.0087 and 0.9994 as peak signal-to-noise ratio (PSNR), structural similarity index, and mean square error (MSE) respectively when compared with Daubechies (59.11 dB, 0.0799, 0.9955), Symlet (56.15 dB, 0.0759,0.9955) and Coiflet (51.61 dB, 0.4978, 0.9758) under the same embedding conditions. The diamond encoding technique, on the other hand, is responsible for the evaluation of all the embeddable regions in the coefficients. The developed system maintained a high payload and imperceptibility with an average PSNR of 65.46 dB and MSE of 0.0244 which are 25.88% and 94.73% improvements over state of the art.

Keywords: Imperceptibility; Integer wavelet transform; Payload; Redundant bits; Sensitive; Steganography.

1. INTRODUCTION

The science and art of hiding information in digital media (video, image, text, and audio) redundant bits for camouflaging purposes is referred to as steganography [1]. Among these digital media used in conveying sensitive information, the digital image is widely used owing to their smaller sizes, availability, a higher rate of withstanding distortion, higher redundant bits, and lower bandwidth requirement when transmitting on the internet [2]. This paper adopted digital image to convey secret images and texts. Generally, steganography information embedding techniques are grouped into time, frequency, and hybrid domains [3]. The time-domain concealing techniques like the diamond encoding (DE), least significant bit amongst others, directly alters the image's pixels and has an advantage of higher payload. However, with high image distortion [4]. which is altered easily [5] when attack. Image steganography has evolved from the direct modification of the digital image bit to the utilization of the frequency domain. Thus, enabling the development of sophisticated schemes that utilize the advantages of robustness and imperceptibility in the frequency domain. The frequency or transform domain such as discrete Fourier transform, discrete cosine transform (DCT), discrete wavelet transform, integer wavelet transform amongst others have been exploited due to their ability to conceal secret information in their frequency coefficients to satisfy imperceptibility and robustness criteria. A steganography system is said to be robust if it is resilient to all attacks that can modify or alter the embedded information [6]. While imperceptibility is the inability in differentiating the image without information and the image with the information referred to as cover-image and stego-image respectively [1]. The mere suspecting of the existence that information exists in a digital image has defeated the purpose of the steganographic system even when the information is not decoded [7, 8]. Unfortunately, the frequency domain is slower due to computational complexity and equally has a lower payload [9]. While the hybrid domain is equally referred to as adaptive or statistics aware concealing techniques and it evaluates the total characteristics of an image before concealing any sensitive information in their transformed coefficients [10].

In the frequency domain, using the DCT requires selecting the coefficient carefully to avoid visible distortion in the stego-image making it computationally complex with a lower payload [11]. The discrete wavelet transform (DWT) was adopted as an alternative owing to as a result of its adaptability and flexibility to represent the digital image signal. Unfortunately, the DWT produces a coefficient with floating-point results when truncated into an integer value (as pixels values are integers) that will destroy the embedded information as the wavelet output coefficients will no longer be integers [12]. The floating-point issue is peculiar to all conventional wavelet transforms as the output of their wavelet filters will not recover the original input

perfectly, thus, making the inverse wavelet transformation to become lossy [7]. Thus, the majority of the transforms in practice are lossy as every computer uses finite precision even in floating-point calculations [13]. Therefore, it is essential to have a transform algorithm to convert integer to integer. Interestingly, the lifting scheme developed by Swedens [14] with the modification of linear transforms has enabled the mapping of input information into integers sub-bands samples using subclasses of general filters banks rounding operators, or quantizers to overcome the floating-point precision problems [13][15]. Unfortunately, this rounding operation introduces quantization noise or error that deteriorates the decorrelation performances [16]. Fortunately, the error is not effective on the signal output provided the signal of the forward output is not modified in the reverse operation [17]. Since an integer wavelet transform is derived from their parent's linear transformation (i.e. DWT), the parent features become important when reducing the errors. Thus, this paper develops a new integer wavelet transform with minimal rounding steps and lifting steps using the most suitable orthogonal wavelet filter. The developed integer wavelet transform is responsible for decomposing digital images into their frequency domain while a DE technique was adopted for evaluating the generated coefficient to conceal the sensitive information. These paper contributions are highlighted as follows.

- Decomposed the classical integer wavelet transform into a non-separable structure with minimal lifting steps and rounding operators
- Performed comparative analysis between the orthogonal wavelet families for the most suitable analyzing and synthesizing filter
- Developed a high payload and imperceptible steganography system.

2. BACKGROUND OF THE STUDY

2.1 Diamond Encoding

There are varying time-domain information concealing techniques presented by researchers among which are the least significant bit (LSB) [5], LSB matching [19], pixel value differencing (PVD), exploiting modification direction (EMD), amongst others [7]. The LSB method due to its simplicity is widely used in hiding information as they alter the least bit in a pixel. Unfortunately, they are detected by any analytical steganography technique [10]. Therefore, the LSB matching became a substitute as it avoids the direct insertion of information and resisted chi-square attacks [11]. The need to increase the embedding payload became the motivation for using EMD and its related types. The relationship between *y* adjacent pixels is used in embedding the sensitive information and became a substitute for LSB matching scheme [18]. The DE uses EMD procedure to conceal $(2l^2 + 2l + 1)$-ary sensitive information in a pixel pair when $l \geq 1$ and it is the concealing parameter [3]. The concealing capacity is l and uses a diamond characteristic value (DCV) matrix. The maximum information in a pixel is $(1/2)\log_2(2l^2 + 2l + 1)$ bit per pixel (bpp) because every pixel in a stego-image carries $\log_2(2l^2 + 2l + 1)$. The smallest concealing value is evaluated using Equation (1) [5]

$$\left\lceil \frac{m \times n}{2} \log_2(2l^2 + 2l + 1) \right\rceil \geq |d_s| \tag{1}$$

where $m \times n$ is the size of the cover image, d_s is sensitive information. The neighborhood set $\varphi(i_j, i_{j+1})$ is determined by Equation (2) as the embedding parameter l is known. The DCV for a pixel pair (r, s) in $\varphi(i_j, i_{j+1})$ is obtained by Equation (3) [19]

$$\varphi(i_j, i_{j+1}) = \left\{(r, s) \left| r - \frac{i_j}{2} \right| + \left| s - \frac{i_{j+1}}{2} \right| \leq l \right\} \tag{2}$$

$$\text{DCV}\ (r, s) = \big((2l + 1)r + s\big) \bmod l \tag{3}$$

The $\varphi(i_j, i_{j+1})$ is the neighborhood set with two characteristics. Firstly, the DCV is unique and not the same even for pixels that are neighbors. More so, a pixel pair (r, s) DCV values are elements of the neighboring set $\varphi(i_j, i_{j+1})$ and within $\{0, 1, 2, \cdots, l - 1\}$. The DCV sets $\varphi(i_j, i_{j+1})$ are evaluated during the concealing of secret information d_s in a pixel pair (i_j, i_{j+1}) to obtain the coordinates $(i_j{}', i_{j+1}{}')$ so that $\text{DCV}\,(i_j{}', i_{j+1}{}') = d_s$. The pixel pair (i_j, i_{j+1}) is later replaced with $(i_j{}', i_{j+1}{}')$. The DE scheme conceals information in (i_j, i_{j+1}) using the values of $\left(\frac{i_j}{2}, \frac{i_{j+1}}{2}\right)$. To prevent underflow/ overflow from happening, it exchanges $i_j{}'$ with $i_j{}''$ and $i_{j+1}{}'$ with $i_{j+1}{}''$ using Equations (4) and (5) [19]:

$$i'' = \begin{cases} i' - s, & i' > 255 \\ i' + s, & i' < 0 \end{cases} \tag{4}$$

$$j'' = \begin{cases} j' - s, & i' > 255 \\ j' + s, & i' < 0 \end{cases} \tag{5}$$

The embedded secret information in the pixel pair (i', j') is obtained by evaluating the DCV of (i', j') using $d_s = \text{DCV}(i', j')$. The DE scheme ensures that any distortion occurring during the concealing process in the pixel pair (i, j) should not be above l.

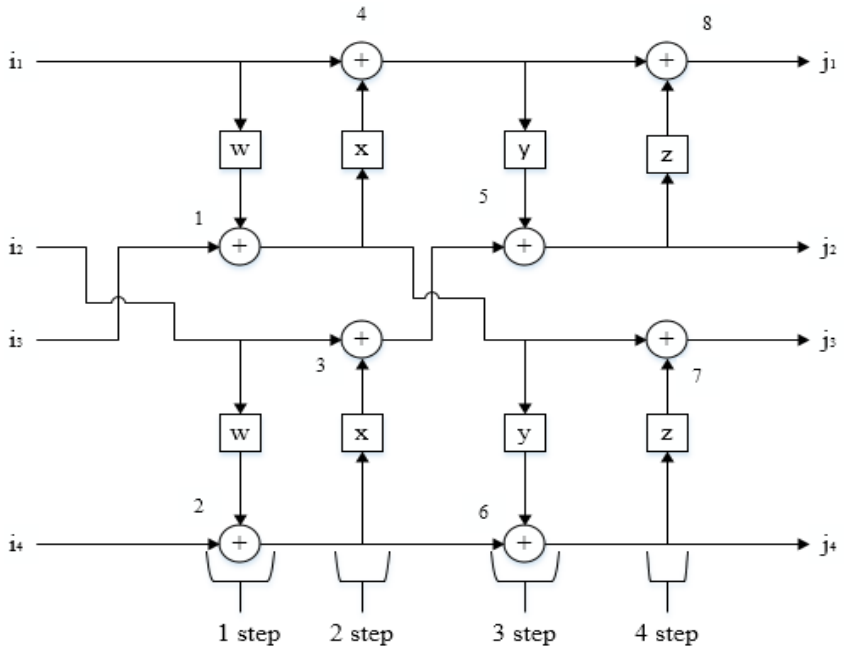


Figure 1. Two dimensional wavelet transform structure [17]

2.2 Integer Wavelet Transform

The integer wavelet transform is obtained from rounding the DWT output as shown in Figure 1. The DWT uses various functions from the wavelet families referred to as the mother wavelet for transformation. The DWT families are grouped into the biorthogonal and orthogonal. The synthesizing and analyzing filters length of an orthogonal wavelet (Daubechies, Haar, Coiflets, and Symlets) are the same whereas the biorthogonal (BiorSplines) wavelet filers vary in length [6]. Other groups are either without scaling function or finite impulse response (FIR) filter or have none. These are: orthogonal wavelets having a scale function (Meyer), complex wavelets without any scale function, and FIR filter (Mexican hat, Morlet, Gaussian, Shannon). The wavelet family varies in various ways such as regularities and smoothness, support lengths, symmetry, coefficients decaying speed, biorthogonality, and orthogonality of the results function [2]. The choice of using the best wavelet transform is essential to achieve effective coding performance since no filter is suitable for all problems. Nevertheless, obtaining the best wavelet transform is usually done through the trials and errors method. However, evaluating each wavelet characteristic will ease the selection procedures. This implies that a tradeoff will be made to obtain the needed advantages.

The lifting scheme allows the new wavelet transforms to be derived from the mother's wavelet using the domain characteristics. The mother wavelet determines the features of the transform obtained, therefore it is important to properly evaluate a proposed application before taking a decision. In steganography, for example, the linear phase assists in phase distortion avoidance during the process of reconstructing the image, lower computation is favored by compact supports. More so, orthonormality eases the convenience of performing analysis. All the aforementioned properties are satisfied by the orthogonal wavelet with various performances that can be verified experimentally to select the most suitable wavelet that will suit steganography [9]. The orthogonal wavelet families do not have any explicit expression except for the Haar wavelet [1]. The wavelet transform generates two coefficient types, wavelet, and scaling coefficients. The scaling coefficient represents the approximated coarse image signal and is derived by averaging two neighboring samples. While subtracting the two neighboring samples will produce a wavelet coefficient to form the fine parts of the image. The scaling and wavelet coefficients of Haar are obtained using Equations (6) and (7) respectively [4].

$$S_n = \frac{i_{2n-1} + i_{2n}}{\sqrt{2}} \tag{6}$$

$$D_n = \frac{i_{2n-1} - i_{2n}}{\sqrt{2}} \tag{7}$$

where S is the scale coefficient, D is the approximated coefficient, i is the image signals and $n = 0,1,2,\ldots,n-1$. Reverse operations are performed to obtain the original image back [20].

3. DEVELOPED SYSTEM

Recall that the conventional two-dimensional (2D) integer wavelet structure presented in Figure 1 has eight rounding operations and four lifting steps. This can further be decomposed into a multi-processing or parallel structure as shown in Figure 2. Contrarily to the classical separable integer wavelet transform in Figure 1, the non-separable 2D integer-to-integer wavelet transforms in Figure 2 allow multiple or parallel processing of any digital input signal at a time. This has the advantage

of lowered lifting steps and rounded operations which reduces the latency of the operation. All steganography transform-domain methods decompose images into detail and approximation coefficients.

Defining:

i - digital image to be encoded
I - image z-transform
r - resolution level
(w, b) - pixel location
$s_r^{(hh)}, s_r^{(lh)}, s_r^{(hl)}, t_r$ - analyzing and synthesizing filters
$i_{r+1}^{(hh)}$ - i diagonal coefficient
$i_{r+1}^{(lh)}$ - i vertical coefficient
$i_{r+1}^{(hl)}$ - i horizontal coefficient
i_{r+1} - i approximation

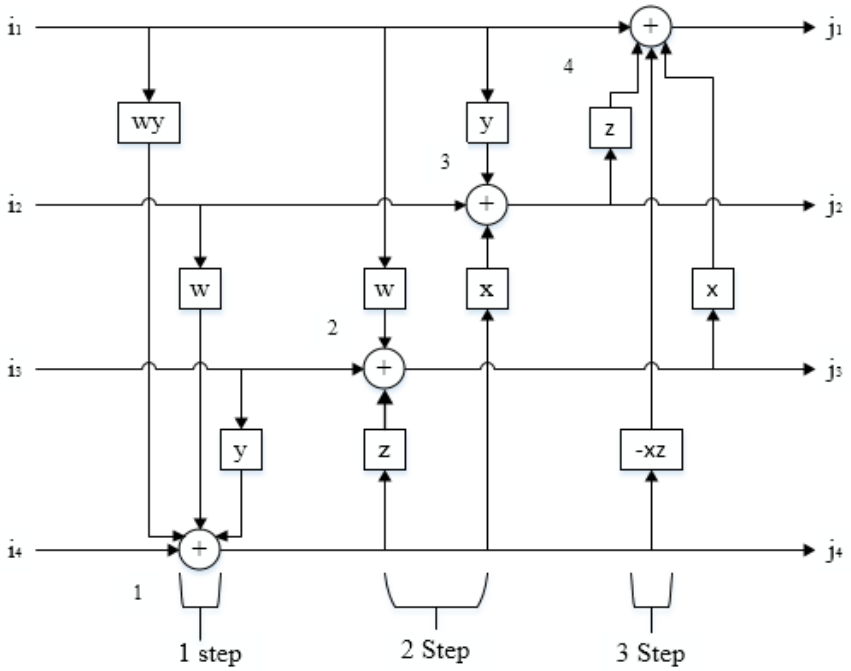


Figure 2. Non-separable 2D integer-to-integer structure

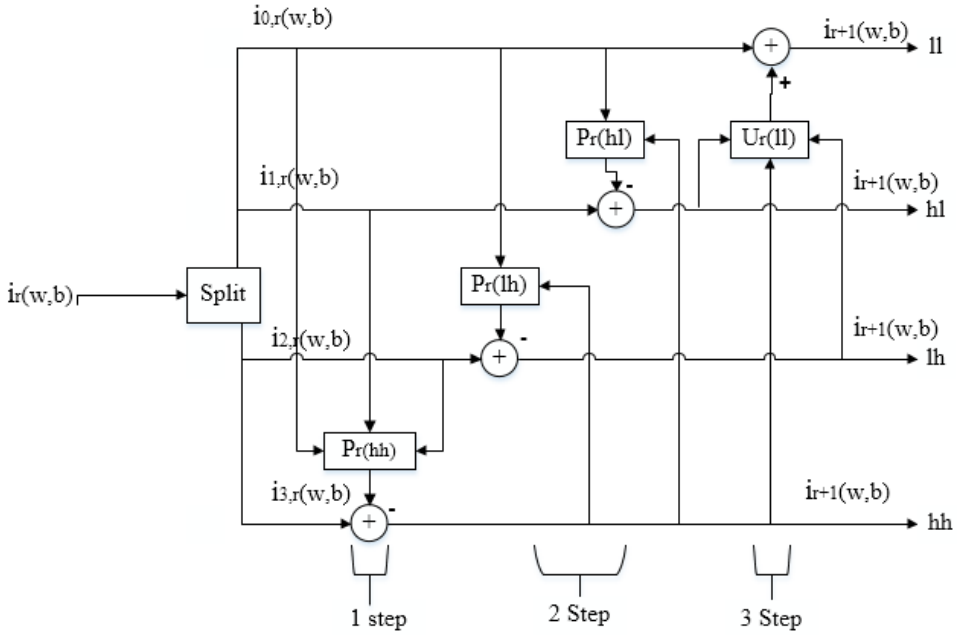


Figure 3. Lifting scheme of 2D of non-separable structure

The coefficients of the 2D non-separable structure detailed and approximation coefficients can be formulated mathematically using Figure 2. In every resolution level r and pixel location level (w, b), the approximation coefficient $i_r(w, b)$ has four polyphase components which can be expressed as

$$i_{0,r}(w, b) = i_r(2w, 2b) \tag{8}$$

$$i_{1,r}(w, b) = i_r(2w, 2b + 1) \tag{9}$$

$$i_{2,r}(w, b) = i_r(2w + 1,2b) \tag{10}$$

$$i_{3,r}(w, b) = i_r(2w + 1,2b + 1) \tag{11}$$

Without any loss of generality, let the input coefficient of the 2D non-separable lifting scheme be the polyphase component. The four analyzing and synthesizing filters are represented as ${s_r}^{(hh)}$, ${s_r}^{(lh)}$, ${s_r}^{(hl)}$ and t_r are used for generating the detail coefficients; $i_{r+1}^{(hh)}$, $i_{r+1}^{(lh)}$, $i_{r+1}^{(hl)}$ and approximate coefficient i_{r+1}. Using the lifting scheme, the 2D non-separable integer-to-integer wavelet transform is restructured as shown in Figure 3.

From Figure 3, the output coefficient can be formulated in the z-transform as follows:

$$i_{r+1}^{(hh)}(z_1, z_2) = I_{3,r}(z_1, z_2) - \left[S_{0,r}^{(hh)}(z_1, z_2)I_{0,r}(z_1, z_2) + S_{1,r}^{(hh)}(z_1, z_2)I_{1,r}(z_1, z_2) + S_{2,r}^{(hh)}(z_1, z_2)I_{2,r}(z_1, z_2)\right] \tag{12}$$

$$i_{r+1}^{(lh)}(z_1, z_2) = I_{2,r}(z_1, z_2) - \left[S_{0,r}^{(lh)}(z_1, z_2)I_{0,r}(z_1, z_2) + S_{1,r}^{(lh)}(z_1, z_2)i_{r+1}^{(hh)}(z_1, z_2)\right] \tag{13}$$

$$i_{r+1}^{(hl)}(z_1, z_2) = I_{1,r}(z_1, z_2) - \left[S_{0,r}^{(hl)}(z_1, z_2)I_{0,r}(z_1, z_2) + S_{1,r}^{(hl)}(z_1, z_2)i_{r+1}^{(hh)}(z_1, z_2)\right] \tag{14}$$

$$i_{r+1}(z_1, z_2) = I_{0,r}(z_1, z_2) - \left[T_r^{(0)}(z_1, z_2)i_{r+1}^{(hl)}(z_1, z_2) + T_r^{(1)}(z_1, z_2)i_{r+1}^{(lh)}(z_1, z_2) + T_r^{(2)}(z_1, z_2)i_{r+1}^{(hh)}(z_1, z_2)\right] \tag{15}$$

Equation (15) is the approximated coefficients of the cover image while Equations (12), (13), and (14) are the detailed coefficients. The DE uses the diamond characteristic value to locate an image embeddable region. Thus, it is employed to embed information in the frequency coefficient. These embeddable regions are $i_{r+1}^{(hh)}$, $i_{r+1}^{(lh)}$, $i_{r+1}^{(hl)}$ and i_{r+1} obtained using Equations (12), (13), (14) and (15) respectively. Since Equation (15) is the approximation of the original cover image, priority is given to $i_{r+1}^{(hh)}$, $i_{r+1}^{(lh)}$ and $i_{r+1}^{(hl)}$ during the embedding phase to maintain a good stego-image. All steganography systems use an embedding algorithm to conceal secret information and also an extraction algorithm to retrieve the secret information. The developed system embedding and extraction algorithm is as highlighted.

3.1 Embedding Algorithm

Let C_O represents the cover-image of size $A \times B$, I_0 represents the secret information and S_0 represents the stego-image. With input, I_0 and output, S_0, the embedding procedures are:

a) Step 1: Convert the I_0 into a binary sequence
b) Step 2: Transform the C_0 into the frequency domain using the developed adaptive non-separable integer-to-integer wavelet transform
c) Step 3: Use Equation (1) to control the embedding process of the binary sequence of I_0
d) Step 4: Use Equation (3) to control the embeddable locations of the sensitive information into $i_{r+1}^{(hh)}$, $i_{r+1}^{(lh)}$, $i_{r+1}^{(hl)}$ and i_{r+1} sub-bands.
e) Step 5: Apply the inverse of the adaptive non-separable integer-to-integer wavelet transform to produce the stego-image S_0 in the spatial domain.

3.2 Decoding Algorithm

The decoding algorithm for retrieving the embedded secret information is as follows:

a) Step 1: transform the S_0 from the time domain into the transform domain using adaptive non-separable reverse integer-to-integer wavelet transform to obtain $i_{r+1}^{(hh)}, i_{r+1}^{(lh)}, i_{r+1}^{(hl)}$ and i_{r+1} sub-bands using the embedded algorithm.
b) Step 2: Scan the $i_{r+1}^{(hh)}$, $i_{r+1}^{(lh)}$, $i_{r+1}^{(hl)}$ and i_{r+1} sub-bands and use the diamond scheme values r and s to extract I_0.

3.3 Comparative Analysis of the Orthogonal Wavelet Family

Since the quality of an image is paramount in steganography, it becomes necessary to evaluate all the orthogonal wavelet families for the most suitable analyzing and synthesizing wavelet filters that will suit the steganography application. Therefore, Haar, Daubechies, Coiflets, and Symlets filter were each chosen to replace both the analyzing and synthesizing filter of the developed system. Lena, beans, baboon pepper Standard images from the Computer Vision Group, University of Granada (CVG-UGR) were chosen for the comparative analysis.

4. RESULTS AND DISCUSSION

The separate processing of 2D signals in the lifting scheme suffers limited processing degrees of freedom due to their formulation from the cascading of a one-dimensional lifting scheme along the horizontal and vertical direction. Thus, the non-separable structure which allows multidimensional memory access was developed and there are compared in Table 1. It is seen that using the non-separable structure in the integer wavelet transform reduces both the rounding operation and lifting steps to 50% and 75% respectively. Thus, the non-separable structure increases the flexibility of the 2D signal processing and equally reduces the latency. Further comparative analysis was performed on Haar, Daubechies, Symlet, and Coiflets, to select the best wavelet filter that will suit the steganography application and the results obtained conveying a sensitive text of 1024 bytes as shown in Table 2.

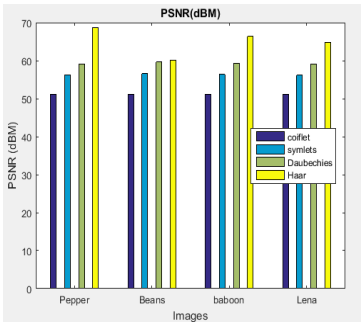
It can be seen in Table 2 that all the embedded information was fully recovered in the four algorithms (AID-Coiflets, AID-Symlets, AID-Daubechies, and AID-Haar). Thus, the match was 100% as shown in Table 2 and this indicated that all the concealed 1024 bytes information were retrieved successfully from the stego-image at varying image quality metrics. The AID-Coiflets have the least PSNR, SSIM, encoding, and decoding time but with the highest mean square error. While the AID-Haar has the highest PSNR, SSIM, encoding time, and the least MSE. This showed that the generated stego-image by the AID-Coiflets algorithm has the highest distortion rate as it has the highest MSE of 0.4978 as seen in Table 2. While the AID-Haar algorithm has the best quality as it has the lowest MSE of 0.0087. Furthermore, the sensitive text size was increased from 1024 bytes to 21456 bytes and concealed in pepper, beans baboon, and Lena standard. The obtained results are presented in Figure 4

Table 1. Comparison of separable and non-separable integer wavelet transform structures

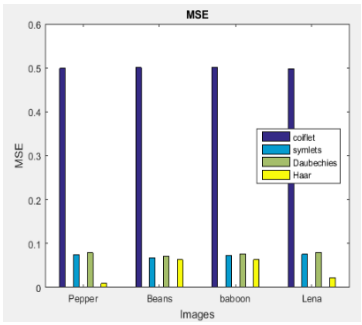
Integer Wavelet Transform	Rounding Operations	Lifting Steps
Separable	8	4
Non-Separable	4	3

Table 2. Evaluation of orthogonal wavelet using image quality metrics

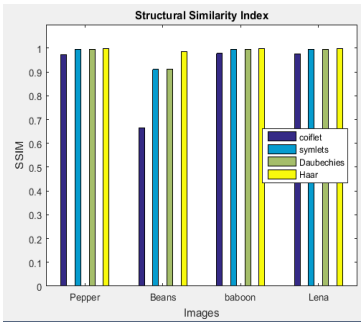
Orthogonal Family	PSNR (dB)	MSE	SSIM	Encode time (s)	Decode time (s)	Match (%)
AID-Coiflets	51.16	0.498	0.996	0.043	0.013	100
AID-Symlets	56.15	0.076	0.995	6.264	2.910	100
AID-Daubechies	59.11	0.080	0.995	5.660	3.118	100
AID-Haar	68.73	0.009	0.999	6.346	0.122	100



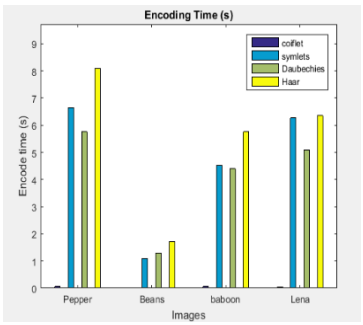
(a) Peak signal-to-noise ratio



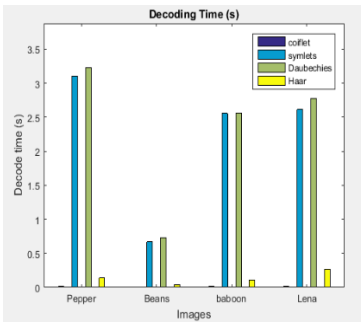
(b) Mean square error



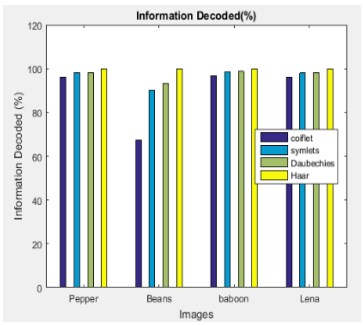
(c) Structural similarity index



(d) Encoding time



(e) Decoding time



(f) Information decoded

Figure 4. Orthogonal wavelet comparison

Figure 4(f) shows that not all the 21456 bytes of secret information embedded into the images by all the algorithms were decoded. Except for the Haar algorithm, the decoded secret information using AID-Coiflets, AID-Symlets, and AID-Daubechies algorithm when compared with the encoded information is lesser than 100%. This indicates that the AID-Haar fully created the highest redundant bits which were able to accommodate all the secret information. However, the AID-Haar has the highest decoding time compared to others as shown in Figure 4€. The reason for the higher embedding time is due to the larger redundant bits created by the Haar. Thus, the increase in the embeddable regions increased the evaluation time by the DE. However, the decoding time of the AID-Haar is reduced due to the Haar wavelet's lower computational time aided by the diamond characteristic value of the DE scheme. For a real-time implementation of steganography in an environment with a high archive of secret information, the high payload becomes the very paramount criterion. From the comparative analysis of all the developed orthogonal wavelet integer-to-integer wavelet transform and DE, it can be generalized that the AID-Haar algorithm has the highest payload, least distortion rate and it is computationally efficient. The reason for this is not farfetched as the linear phase in image processing aid the avoidance of any phase distortion during the formation of an image. Furthermore, computational efficiency is aided by compact supports and orthonormality ease in performing analysis conveniently. Nevertheless, no filter bank or two-band wavelets except the Haar functions satisfies these demands as proven by Daubechies [9]. Therefore, this paper adopted the Haar as the analyzing and synthesizing filter for the developed system.

To effectively assess the performances of the developed system with the state of the art, different cover images obtained from CVG-UGR images datasets [1] were used to covey different secret data of varying sizes and their performances compared with the works of [1] a shown in Table 3. It can be seen that the developed system had a higher PSNR, structural similarity index (SSIM), and lowest MSE when compared with the state of the art. This indicated that the developed system has a higher payload and is equally highly imperceptible.

Table 3. Statistical performances of various secret-image (192 × 192) using cover-images (256 × 256)

	Kadhim *et al.* [1]			AID System		
Cover-image	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Lena	51.40	0.4709	0.9993	62.10	0.0401	1.0000
Mandrill	51.83	0.4268	0.9995	67.62	0.0112	1.0000
Pepper	51.80	0.4300	0.9991	67.96	0.0104	1.0000
Airplane	53.32	0.3031	0.9997	66.77	0.0137	0.9997
Lake	52.17	0.5407	0.9994	65.72	0.0174	1.0000
Car	52.43	0.7316	0.9996	70.85	0.0054	0.9988
Splash	51.13	0.4866	0.9990	67.61	0.0113	1.0000
House	51.70	0.4389	0.9993	60.70	0.0554	1.0000
Tree	52.12	0.3987	0.9995	60.54	0.0575	0.9982
Couple	52.06	0.4022	0.9995	64.71	0.0220	0.9992
Average	52.00	0.4630	0.9994	65.46	0.0244	0.9996

5. CONCLUSION

This paper has presented a high payload and imperceptible steganography system to suit high payload applications such as sensitive office documents records, electoral results storage and sharing, patients' health information management system, amongst others. It is essential to subject any new steganography technique to various attacks to evaluate the effect of such attacks on the embedded secret information. Thus, this paper tends to subject the developed system to various attacks in its future work.

REFERENCES

[1] I. J. Kadhim, P. Premaratne and P. J. Vial, High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research,* 60, 2020, 20-32.

[2] A. A. Attaby, M. F. M. Ahmed and A. K. Alsammak, Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3, *Ain Shams Engineering Journal*, 9(4), 2018, 1965-1974.

[3] D. Laishram and T. Tuithung, A survey on digital image steganography: Current trends and challenges, *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, Jaipur, India, 2018.

[4] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho and K. -H. Jung, Image steganography in spatial domain: A survey, *Signal Processing: Image Communication,* 65, 2018, 46-66.

[5] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan and M. Sajjad, CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method, *Multimedia Tools and Applications,* 76(6), 2017, 8597-8626.

[6] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari and B. Gupta, Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain, *Multimedia Tools and Applications,* 76(18), 2017, 18451-18472.

[7] M. A. Idakwo, M. B. Muazu, E. A. Adedokun and B. O. Sadiq, An extensive survey of digital image steganography: State of the art, *ATBU Journal of Science, Technology and Education*, 8(2), 2020, 40-54.

[8] H. N. Abed, N. H. Hassoon, A. L. Ahmed and I. S. Albayaty, Hiding information in an image based on bats algorithm, *Iraqi Journal of Information Technology,* 8(2), 2018, 128-141.

[9] J. Kaur and S. Pandey, An adaptive quad tree based transform domain steganography for textual data, *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 2017.
[10] M. S. Subhedar and V. H. Mankar, Current status and key issues in image steganography: A survey, *Computer Science Review*, 13, 2014, 95-113.
[11] P. Vanathi, Reversible data hiding based on radon and integer lifting wavelet transform, *Informacije MIDEM: Journal of Microelectronics, Electronics Components and Materials,* 47(2), 2017, 91-100.
[12] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti and R. Logesh, SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images, *Measurement*, 139, 2019, 426-437.
[13] H. Chao and P. Fisher, *An Approach to Fast Integer Reversible Wavelet Transforms for Image Compression*, 1996.
[14] S. A. Seyyedi, V. Sadau and N. Ivanov, A secure steganography method based on integer lifting wavelet transform, *International Journal of Network Security,* 18(1), 2016, 124-132.
[15] L. Xiong, Z. Xu and Y. -Q. Shi, An integer wavelet transform based scheme for reversible data hiding in encrypted images, *Multidimensional Systems and Signal Processing,* 29(3), 2018, 1191.
[16] T. Strutz and I. Rennert, Two-dimensional integer wavelet transform with reduced influence of rounding operations, *EURASIP Journal on Advances in Signal Processing,* 2012, 75.
[17] F. A. B. Hamzah, T. Yoshida, M. Iwahashi and H. Kiya, Channel scaling for rounding noise reduction in minimum lifting 3D wavelet transform, *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, Hong Kong, 2015.
[18] C. -S. Tsai, H. -C. Wu, C. -C. Lee, T. -F. Shie and C. -C. Lee, A steganographic method by pixel-value differencing and exploiting modification direction, *Journal of Computers,* 28(1), 2017, 13-29.
[19] Y. -B. Ma, Q. -S. Wen, Z. -M. Lin and T. -S. Chen, A high visual quality embedding method in edges based on pixel pair difference, *Proceedings of the 8th International Conference on Mobile Multimedia Communications*, Chengdu, China, 2015.
[20] R. Reisenhofer, S. Bosse, G. Kutyniok and T. Wiegand, A Haar wavelet-based perceptual similarity index for image quality assessment, *Signal Processing: Image Communication,* 61, 2018, 33-43.