Robust Steganography Technique for Embedding Secret Images

Nehayat Ezzaldeen Majeed [1], Haval Mohammed Sidqi [2]

Department of Applied Computer, College of Applied and Medical Sciences, Charmo university, Chamchamal City, Kurdistan Region, Iraq

Department of Information technology, College of Informatic, Sulaimania Polytechnic University, Sulaymaniyah City, Kurdistan Region, Iraq

Corresponding author's e-mail:nehayat.ezzaldeen@charmouniversity.org

Abstract

Steganography is a technique used to disguise the existence of a secret communication. It is used in many fields to solve information security problems. Steganography is a technique to embed secret data in a carrier image and obtain a new image that can't actually be distinguished from the original image. This paper proposes steganography method based on least significant bit (LSB) replacement and integer wavelet transform IWT through lifting scheme to achieve high quality of stego image. we will do some pre-processing on the secret image before embedding process. IWT transforms the secret image from spatial domain to a frequency domain and will be divided it into a group of sub-bands, some of which we will use for their utmost importance and ignore some of them.

We have embedded the secret image in a sequential LSB method and in a randomly LSB method and also by the method LSB matching. But after applying our proposed method to the secret image and then embedded it in each of the three above-mentioned methods, it was found that it had a higher degree of imperceptibly and obtained a higher rate of PSNR and the possibility of recovering the secret image without errors. By using the randomly and LSBM methods gives a higher security and resistance to extraction by attackers.

Keywords: Integer Wavelet Transform (IWT), LSB Steganography, Peak Signal-to-Noise Rate (PSNR), Cover image, Mean Squared Error (MSE).

گۆڤاری زانکۆی هەڵەبجە:گۆڤاریێکی زانستی ئەکادیمیە زانکۆی هەڵەبجە دەری دەکات	
DOI Link	http://doi.org/10.32410/huj-10443
ڕێککەوتەکان	ڕێکەوتی وەرگرتن: ٢٠٢٢/٨/٦ | ڕێککەوتی پەسەندکردن: ٢٠٢٢/٩/٢٢ | ڕێککەوتی بڵاوکردنەوە: ٢٠٢٢/١٢/٣٠
ئیمەیلی توێژەر	nehayat.ezzaldeen@charmouniversity.org
مافی چاپ و بڵاوکردنەوە	©٢٠٢٢ نیهایەت عزالدین مەجید ، پ.ی.د. هەڤاڵ محەمەد صدیق، گەیشتن بەم توێژینەوەیە کراوەیە لەژێر ڕەزامەندی CCBY-NC_ND 4.0

الملخص

علم إخفاء المعلومات هو أسلوب يستخدم لإخفاء وجود اتصال سري. يتم استخدامه في العديد من المجالات لحل مشاكل أمن المعلومات. Steganography هي تقنية لتضمين البيانات السرية في الصورة الحاملة والحصول على صورة جديدة لا يمكن تمييزها فعليًا عن الصورة الأصلية. يقترح هذا البحث طريقة إخفاء المعلومات التي تعتمد على الاستبدال الأقل أهمية للبت ((LSB وتحويل عدد صحيح من الموجات المويجة IWT من خلال مخطط الرفع لتحقيق جودة عالية لصورة .stegoسنقوم ببعض المعالجة المسبقة على الصورة السرية قبل عملية التضمين. تقوم IWT بتحويل الصورة السرية من المجال المكاني إلى مجال التردد وسيتم تقسيمها إلى مجموعة من النطاقات الفرعية ، والتي سنستخدم بعضها لأهميتها القصوى ونتجاهل بعضها.

قمنا بتضمين الصورة السرية بطريقة LSB المتسلسلة وطريقة LSB بشكل عشوائي وأيضًا بطريقة مطابقة .LSBM ولكن بعد تطبيق طريقتنا المقترحة على الصورة السرية ثم تضمينها في كل من الطرق الثلاث المذكورة أعلاه ، تبين أنها تتمتع بدرجة أعلى من عدم الإدراك وحصلت على نطاق أعلى من PSNR وإمكانية استعادة الصورة السرية بدون أخطاء. باستخدام الأسلوب العشوائي وطريقة LSBM يعطي أمانًا ومقاومة أعلى للاستخراج من قبل المخربين.

الكلمات المفتاحية: التحويل المويجي الصحيح، اخفاء المعلومات بت الأقل دلالة ، ذروة الإشارة إلى نسبة الضوضاء، صورة الغلاف، متوسط الخطأ التربيعي.

پوختە

ستێگانۆگرافی تەکنیکێکە بۆ شاردنەوەی بوونی پەیوەندییەکی نهێنی. لە زۆر بواردا بەکاردێت بۆ چارەسەرکردنی کێشەکانی ئاسایشی زانیاری. ستێگانۆگرافی تەکنیکێکە بۆ شاردنەوەی زانیاری نهێنی لە وێنەیەکی هەڵگردا و بەدەستهێنانی وێنەیەکی نوێ کە لە ڕاستیدا ناتوانرێت لە وێنەی ڕەسەن جیا بکرێتەوە. ئەم توێژینەوەیە پێشنیاری شێوازێکی ستێگانۆگرافی دەکات کە پشت بە کەمترین کاریگەری بیت (LSB) و گۆڕینی شەپۆلی ژمارە تەواوەکان IWT دەبەستێت لە ڕێگەی نەخشەی بەرزکردنەوە بۆ بەدەستهێنانی وێنەی ستیگۆی کوالێتی بەرز. ئێمە چەند پرۆسێسێکی پێش چارەسەر دەکەین لەسەر وێنەی نهێنی پێش پرۆسەی شاردنەوە. IWT وێنەی نهێنی لە دۆمەینی فەزاییەوە دەگۆڕێت بۆ دۆمەینی فرێکوێنسی ودابەشی دەبێت بۆ کۆمەڵێک باندی لاوەکی، کە هەندێکیان بۆ ئەوپەڕی گرنگیان بەکاری دەهێنین و بەشێکیان پشتگوێ دەخەین.

ئێمە بە تەکنیکی هەڕەمەکی وێنەی نهێنیمان لە زنجیرەی (LSB) شاردەوە. وە هەروەها بە تەکنیکی زنجیرەیی (LSB) یش شاردمانەوە. وە بە شێوازی (LSBM) ی لە یەک چوو شاردمانەوە، بەڵام دوای بەکارهێنانی شێوازی پێشنیارکراوی ئێمە بۆ وێنە نهێنییەکە و پاشان شاردنەوەی بە هەریەکێک لەو سێ شێوازەی سەرەوەدا، دەرکەوت کە پلەیەکی بەرزتری بە شێوەیەکی هەستپێنەکراوی هەبوو ومەودای بەرزتری PSNR و ئەگەری وەرگرتنەوەی وێنە نهێنییەکەی بەدەستهێناوە بەبێ هەڵە. بە بەکارهێنانی شێوازەکانی هەڕەمەکی و LSBM ئاسایش و بەرگرییەکی بەرزتر دەدات لە دەرهێنان لەلایەن تێکدەرانەوە.

وشە کلیلییەکان: گۆڕینی شەپۆلی ژمارە تەواوەکان، ستێگانۆگرافی کەمترین کاریگەری بیت، لوتکەی سیگنأل بۆ ڕێژەی ژاوەژاو، وێنەی بەرگ، هەڵەی چوارگۆشەی مامناوەند.

1 Introduction

Steganography is the art and science of concealing communication. steganographic systems embed secret information in routine cover media to avoid drawing attention from potential hackers (Provos & Honeyman, 2003). There are many examples of Steganography such as sending a message to a spy by distinguishing special letters in a newspaper using invisible ink and add intangible echo at specific locations in audio recording (Petitcolas, Anderson, & Kuhn, 1999). Steganography can be implemented electronically by putting a secret message (a binary file) within some sort of cover (video, text, sound or image file) and as a result obtained a “stego-object”. The stego-object is originally the cover file with its least significant data replaced with the secret message (Hempstalk, 2006). The main goal of hiding information in image steganography is to reduce the difference between cover image and stego image so that it can be hidden the existence of any confidential communication and transmit the information invisibly. The steganography methods are evaluated by four parameters which are payload capacity, imperceptibility, security and robustness (Shah & Bichkar, 2018). In image steganography the pixels values are converted from the decimal system to binary and then the least significant bits (LSB) of the cover image are changed with the secret message bits to obtain the stego image (Mielikainen, 2006). So that the enemy cannot extract the secret bits, it is preferable to choose a random permutation method to hide the secret data in the cover image as a function of a secret key (Aura, 1996). Spatial domain and transform domain embedding in image steganography are the two most popular methods. Spatial domain algorithms implement the process of embedding directly on the cover image to hide the secret image. They are faster and simple, however they are vulnerable to compression and distortions. The techniques used like Least Significant Bit (LSB), Pixel Value Differencing (PVD), Exploiting Modification Direction (EMD). Domain-transforming algorithms first change the cover image into another format then apply the embedding process on the new format, these new formats are to convert the cover image into four smaller sub-bands. These procedures are resistant to compression and distortion, However, they require expensive computations (Ahmad, et al., 2022). They use strategies like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Fast Fourier Transform (FFT) (Ahmad, et al., 2022). LSB matching technique provides better security for the secret message because more bit modification is produced by matching. Even so, it's possible that all the bits will need to be altered. As a result, the pixel value is randomly increased or decreased by 1, eliminating the asymmetry of odd and even Pixels (Maiti, Nayak, & Sarkar, 2017).

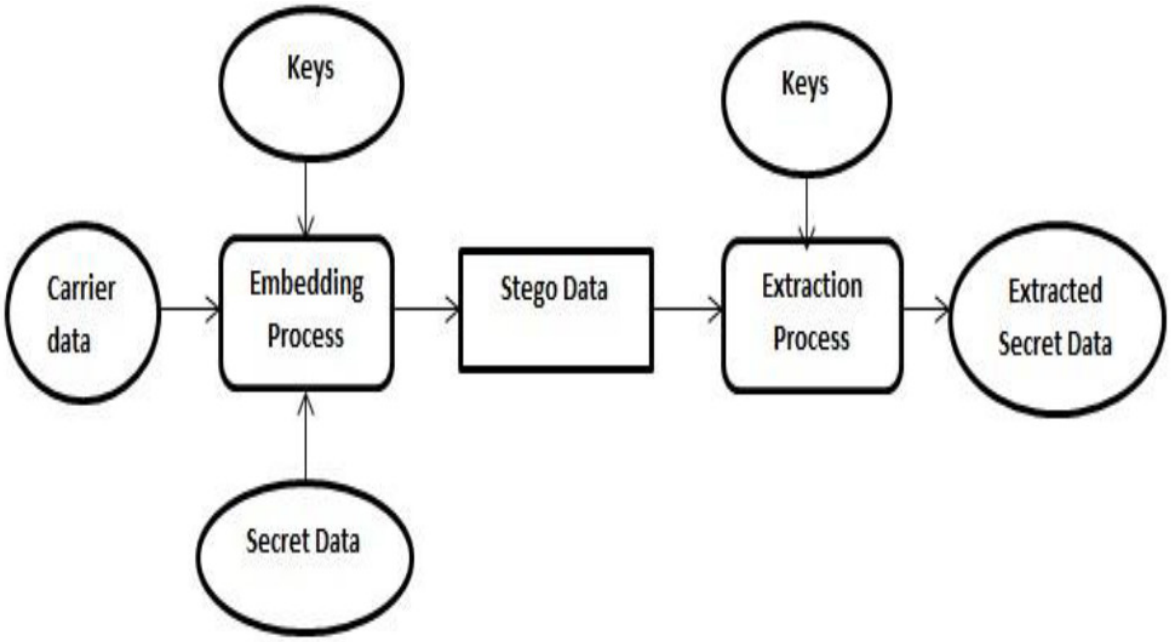

Figure 1. Steganography Process (Kaur & Rani, 2016)

The most popular metrics used to assess the quality of the image are the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics. MSE (mean squared error) is the total of the squared values of the overall differences between the original and stego images, divided by the size of the images. Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible signal strength and the amount of decreasing noise that interferes with the signal's representation (Gutub & Al-Shaarani, 2020).

This paper suggested a new method for embedding the gray image inside another gray image. This method depended on applying integer wavelet transform IWT to the secret image and using the low-frequency sub-bands which are obtain in the first and second levels in embedding process and use PSNR and MSE for measuring the quality of the stego image.

2 Related Work

In (Abdul-Sada, 2007), An approach in the spatial domain has been suggested. The Third Least Significant Bit (LSB-3) of the cover image has been utilized to hide the message bits, and LSB-1 and LSB-2 may be adjusted according to the message bits to reduce the variance between the stego-cover and the cover. This is the main idea behind the suggested method. A stego-key has been utilized to permute the message bits before embedding them for added security. The findings of this approach, however, revealed that the LSB -1 method has greater PSNR values than that of the suggested way, indicating that the LSB -1 image has superior quality than the modified one while maintaining the same capacity.

In (Wang, Tang, & Wang, 2020), A hybrid steganography technique based on LSB replacement and Hamming

code (HLAH) is suggested. Since the sharp edges of the image can withstand more alterations than the smooth parts, more hidden messages are placed there, and less information is placed in the smooth areas of the image. Peak signal-to-noise ratio (PSNR), mean square error (MSE), Payload capacity and histogram analysis were used to gauge how well the suggested HLAH approach performed. Their test findings demonstrated that the suggested HLAH method not only has a higher embedding capacity than other methods currently in use, but also provides better image quality.

In (Chan & Cheng, 2004), a data concealing method using straightforward LSB substitution is suggested. The image quality of the stego-image can be significantly enhanced with minimal additional computing cost by using an optimal pixel adjustment process to the stego-image created by the straightforward LSB substitution method. The worst case mean-square error between the cover image and the stego image was calculated. Their test findings demonstrated that the stego-image and the original cover-image are visually identical.

In (Shah & Bichkar, 2018), the idea of spatial domain image steganography is presented. They used acceptable sites to hide 2 bits of secret data in each pixel, resulting in the development of coefficients corresponding to the location of match, to hide a stream of secret data in a quarter of the image. These coefficients were concealed using LSB replacement steganography in the remaining portion of the image. To locate the most effective place in the image to conceal these coefficients, scientists utilized a genetic algorithm. They compared the suggested technique's results to those of LSB replacement steganography and found that the proposed technique is significantly better than LSB steganography. It gives improvement in values of MSE and PSNR.

Two metrics that are frequently used in evaluating the quality of images are peak signal to noise ratio (PSNR) and structural index similarity (SSIM). In (Setiadi, 2021) is a study that attempts to review, validate, and analyze the PSNR and SSIM measurement data on three different methods, including LSB, PVD, and CRT. According to the test results, LSB have the highest values based on PSNR and PVD have the highest values based on SSIM. In LSB and CRT than in PVD, the variations based on the histogram are more obvious. When compared to PSNR, results from other analyses, such as RS attack, were similarly more consistent with SSIM readings. They came to the conclusion that SSIM is a more accurate indicator of imperceptibility overall.

In (Zhu, et al., 2020), Block compressive sensing (BCS) and singular value decomposition (SVD) embedding are used to provide an effective and reliable meaningful image encryption (MIE) technique. The simple image is first divided equally and sparsely represented in the discrete cosine transform (DCT) domain. The coefficient vectors are then randomly permuted (CRP) to create confusion, and compressive sensing is used to encrypt the coefficient vectors into a secret image. The final meaningful cipher image is then produced by using SVD embedding to incorporate the secret image into a carrier image. For the purpose of proving the confidentiality, effectiveness and robustness of the suggested scheme, simulation results and thorough performance assessments are offered.

In (Chen, et al., 2021), mentioned a suggested approach for converting an image into a carrier image with visual meaning. They put forth an enhanced approach based on the integer wavelet transform (IWT) and prediction scheme, which was inspired by the visually secure encryption methodology. To increase the quality of the final image, prediction error is employed to permute the carrier image's pixels and the secret image is concealed in the high frequency coefficients of IWT to produce good invisibility. The quality of the encrypted image is 3.5 dB better than that of the earlier ones, according to experimental findings and analysis.

In (Subhedar & Mankar, 2019), introduced a novel image steganography method based on framelet transforms that conceals a secret image within a cover image. They obtained the stego image by embedding the hidden information in singular framelet coefficient values. According to simulation studies, stego images have greater visual quality and are resistant to a number of common image processing techniques. The security performance of the suggested method examined utilizing a variety of steganalysis techniques. All cases have low detection accuracy, which supports the undetectability.

In (Ker, 2004), have a looked at techniques for reliably determining whether an image includes concealed data; They focused on grayscale bitmap images and straightforward LSB steganography. They have extensively assessed the dependability of several steganalysis techniques using a distributed computer network and a library of more than 30,000 images. The findings pointed to a number of enhancements to the conventional techniques. Extensive testing demonstrated that the enhanced techniques enable accurate LSB steganography identification with embedded messages that are between 2 and 6 times smaller.

3. Proposed method

The integer wavelet transform is utilized in this section. So, before going into detail about our approach, let's quickly go through the wavelet transform and its features.

3.1 Integer Wavelet Transformation (IWT)

In this paper, we are applied the integer wavelet transform for avoid using floating point coefficients. This transform is an integer to integer mapping, and a well-known retrievable transform in this category is the Haar lifting transform. The transform and inverse transform are depicted in equations (1) and (2), respectively:

$$D_{1,n} = S_{0,2n+1} - S_{0,2n} \quad \text{.....(1)}$$

$$S_{1,n} = S_{0,2n} + (D_{1,n})/2$$

$$S_{0,2n} = S_{1,n} - (D_{1,n})/2 \quad \text{..... (2)}$$

$$S_{0,2n+1} = D_{1,n} + S_{0,2n}$$

where Si,n, and Di,n, are the n-th low and high frequency coefficients of the wavelet in i-th level, respectively. Four distinct matrixes will be produced when an image is transformed using this method. The first one is an approximation matrix (LL), which resembles the input image but is scaled down. The three other matrixes (LH, HL, HH) display the details of the original image in different directions (Miri & Faez, 2018). The results of Lena's integer transform are displayed in Figure 2. The high frequency coefficients of the Lena picture are depicted in the Figure as LH, HL, and HH.

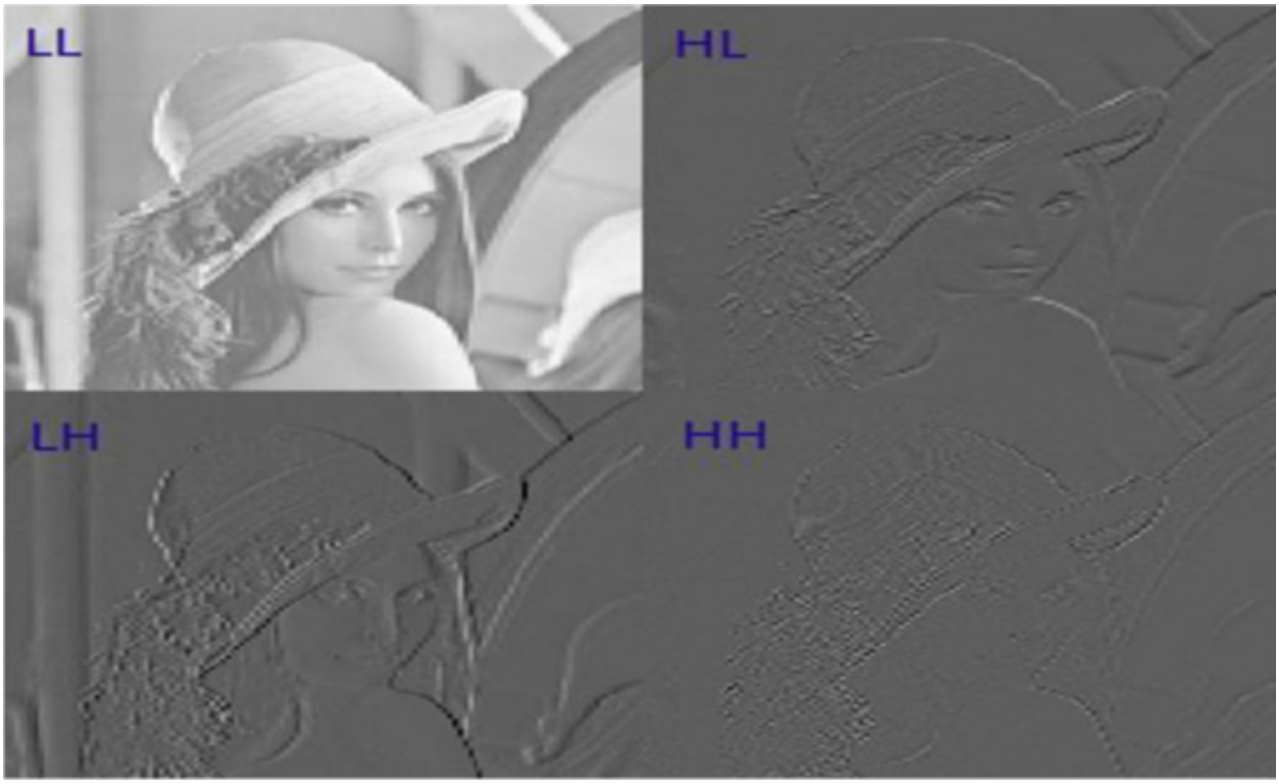

Figure 2. Approximation and detail matrixes of Lena image (Miri & Faez, 2018)

3.2 Proposed technique based on integer wavelet transform IWT

In our method, we are applied integer wavelet transform IWT on the secret image and obtained in the first level four sub-bands (LL, LH, HL, HH). Then in the second level we applied IWT on the sub-band (LL) and it was decomposed into another four sub-bands (LL_LL, LH_LL, HL_LL, HH_LL). Since these bands are within the low frequency sub-band (LL) which is an approximate matrix and similar the original image but as a smaller version, they are contain the most important information, so we kept them as they are, then we are applied inverse integer wavelet transform (IIWT) on the four sub-bands which are obtained from the sub-band (LL). We are applied IWT to the sub-band (LH) and got the sub-bands (LL_LH, LH_LH, HL_LH, HH_LH), we are kept the sub-bands (LL_LH, LH_LH) because they are containing more information, and zeroing the sub-bands (HL_LH, HH_LH) because they are fall within the high frequency and containing less information, then we are applied inverse integer wavelet transform (IIWT) on the four obtained sub-bands from the sub-band (LH).

In the same way for the sub-band (HL) we are applied IWT and got (LL_HL, LH_HL, HL_HL, HH_HL), here we are kept the two sub-bands (LL_HL, HL_HL) and zeroing the two sub-bands (LH_HL, HH_HL), then implementing (IIWT) on them.

Also, the sub-band (HH) was decomposed into four sub-bands by applying IWT to it and they are (LL_HH, LH_HH, HL_HH, HH_HH). HH matrix is the highest frequency detail of the input image, and it contain the least important information, so we zeroed all its sub-bands and then applied (IIWT) to them.

Thus, we became have sixteen sub-bands, of which we have kept eight of the low frequencies and zeroed the other eight of the high frequencies, as shown in figure 3 (a and b).

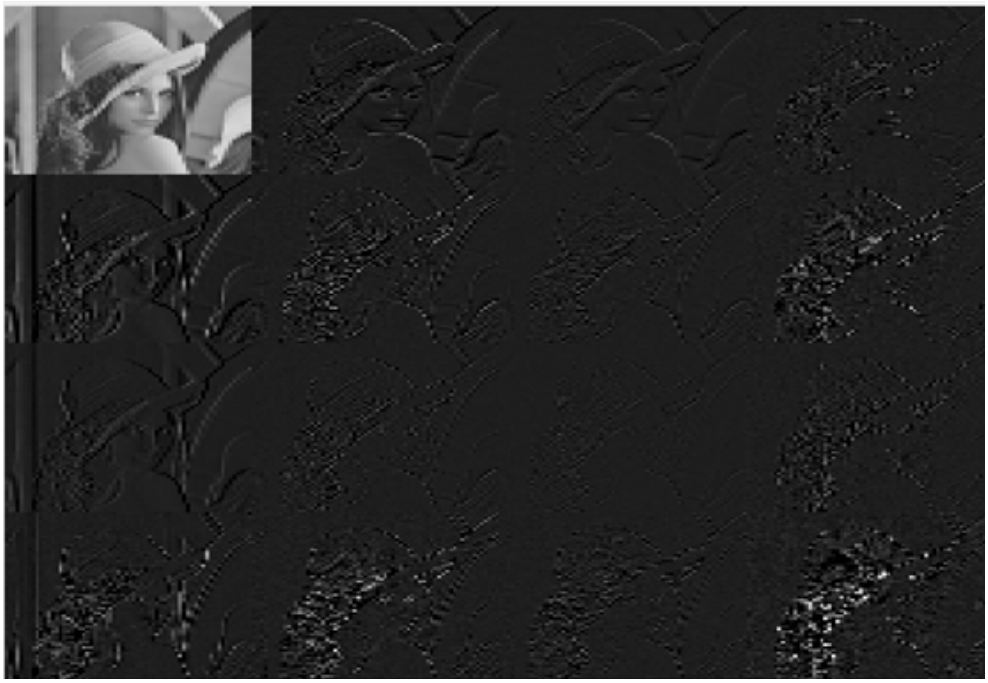

Figure 3. (a) After divided into 16 sub-bands by applying IWT for each sub-band

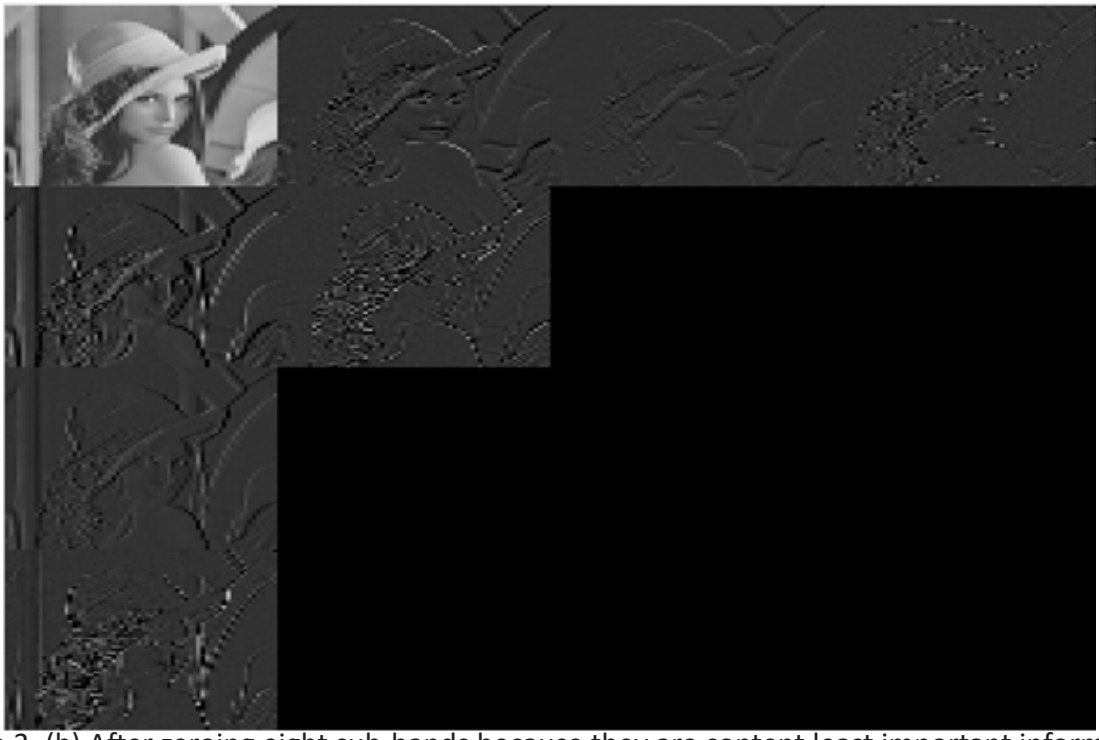

Figure 3. (b) After zeroing eight sub-bands because they are content least important information

For reconstructed the image we implemented (IIWT) for each of (IIWT for LL), (IIWT for LH), (IIWT for HL) and (IIWT for HH). We obtained the secret image as shown in figure 4. (b)

(a) (b)

Figure 4. (a) Secret image, (b) Secret image after implemented our technique

We embedded the secret image before and after applying our method to it in the cover image with LSB Sequential Substitution, LSB Random Replacement, and LSB Matching One Bit Per Pixel techniques. The stego-image that we obtained by our method had higher quality, the results that we obtained through the application using the Matlab program and presented in the tables in the results section is proof of that. figure 5. shows the stego-image for our proposed in LSB sequential and stego image for LSB usual sequential.

(a) (b)

Figure 5. (a) Stego image for our proposed in LSB randomly technique, (b) Stego image for LSB usual randomly

When applying IWT on the secret image the coefficients values in the sub-bands are positive and negative, and in order for all the values to become positive, we find the lowest value of each sub-band, which is a negative value, and then add the absolute value of the lowest value to all the coefficients values in that sub-band. Sometimes some values become greater than 255, so it needs nine bits, and sometimes it becomes greater than 511, then it needs ten bits, so all values for that sub-band must be represented by nine or ten bits. Here the number of bits will be increased and this leads even to a small percentage to reduce the quality of the stego image, this is considered as the disadvantage of our method.

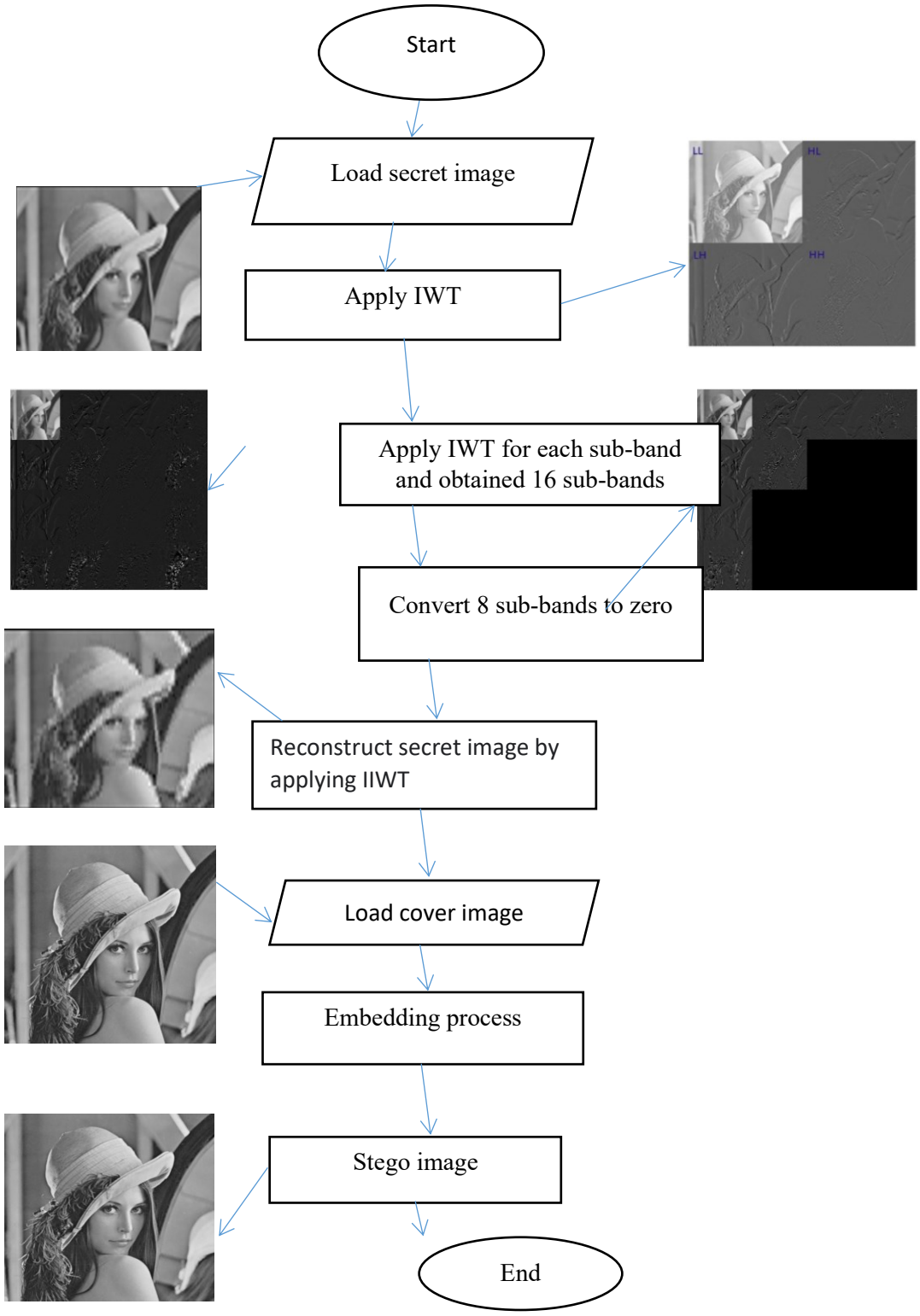

Figure 6. Diagram of Embedding process

3.3 Extraction process

When extracting secret bits from the stego image, they must be divided into eight groups. Each group represents the secret bits of one sub-band. Then converting bits from binary system to decimal number that is coefficients values. the coefficients values of each sub-band must be added to the smallest value of that

sub-band after the second level of IWT is applied and divided the image into eight sub-bands, and in this way the coefficients values return to their original values.

After specifying the coefficients values of the sub-bands, we choose any image with the size of the secret image and we zeroing it completely and then apply integer wavelet transform (IWT) to it and obtain (LL, LH, HL, HH), then apply (IWT) to each sub-band and we become have sixteen sub-bands. Now we put each specific group of coefficients in its sub-band in the sequence chosen by the sender. Then by applying inverse integer wavelet transform (IIWT) to the four bands of (LL), which is (LL_LL, LH_LL, HL_LL, HH_LL) and to the four bands of (LH), and (HL), and (HH). Finally, implementing (IIWT) for each of (inverse LL, inverse LH, inverse HL, inverse HH) to reconstruct the secret image. In this way we can extract the secret image without any error.

4 Experimental Results and Discussion

To perform experiment, we have selected the dataset USC-SIPI (University of Southern California-Signal and Image Processing Institute), grey scale images. An assortment of digitized images can be found in the USC-SIPI image database (Weber, 2018). We used 44 images. It is largely maintained to facilitate research in machine vision, image analysis, and image processing. We used Lina's image (256*256) as the cover image. And we used the (44) images as secret images with a size of (64 * 128). To perform experimentation, MATLAB (R2017a) on Intel core i7 was used. Figure 6 secret images.

Figure 6. Secret images

PSNR and MSE are the standard measures is typically used to assess how similar the original image and stego image The mean squared error (MSE), which is computed of the squared intensity differences of distorted and reference picture pixels, is the most popular and simplest full reference measure. When PSNR value is high that indicates that the cover image has small distortion after embedding. But when PSNR value is low that represents poor visual quality of the cover image. Eqs. 3 and 4, M and N are representing the whole number of rows and columns in the image, respectively, yield the MSE and PSNR of stego-images. Xij and Yij are, respectively, the pixel values of the ijth location of the original image and the stego-image. (Pratik , D Shah ; R, S Bichkar, 2018).

PSNR and MSE are the standard measures is typically used to assess how similar the original image and stego image The mean squared error (MSE), which is computed of the squared intensity differences of distorted and reference picture pixels, is the most popular and simplest full reference measure. When PSNR value is high that indicates that the cover image has small distortion after embedding. But when PSNR value is low that represents poor visual quality of the cover image. Eqs. 3 and 4, M and N are representing the whole number of rows and columns in the image, respectively, yield the MSE and PSNR of stego-images. Xij and Yij are, respectively, the pixel values of the ijth location of the original image and the stego-image. (Pratik , D Shah ; R, S Bichkar, 2018).

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2 \qquad \text{.....(3)}$$

PSNR = 10. Log10 (255)2 /MSE ..... (4)

After we implemented our method on the secret images, we measured PSNR between it and the original secret images, and the results were as in Table (1).

Table (1) PSNR Between the original secret images before any pre-processing and the reconstruct secret images after implementing our method

No. of images	PSNR
1	34.3307
2	34.5473
3	36.8275
4	35.0487
5	33.4193
6	28.3652
7	33.8979
8	30.9012
9	32.4424
10	33.9603
11	31.0689
12	29.4661
13	29.5096
14	28.5702
15	29.8043
16	35.2696
17	27.2157
18	33.5954
19	30.9586
20	27.0026
21	29.1914
22	33.5367
23	27.4382
24	30.3362
25	28.6576
26	31.8031
27	35.3107
28	32.8229
29	36.119
30	35.4945
31	33.0759
32	33.0696
33	33.8942
34	37.8323
35	35.558
36	35.3715
37	34.9638
38	30.8005
39	30.4276
40	54.7825
41	30.3951
42	24.6001
43	36.8526
44	30.4447

Average 32.7041

As we mentioned earlier, we implemented the sequential LSB replacement and, randomly LSB replacement and also with the method LSB matching replacement for all images by one bit per pixel, and then after applying our method to all secret images, we embedded them in the cover image by the three methods. We compared the results and our method had a higher average of PSNR in each of the three methods. Table 2 shows sequential LSB replacement and our method in sequential LSB replacement.

Table (2) PSNR by sequential LSB and our proposed in sequential LSB

PSNR (LSB sequential)		PSNR (our proposed LSB sequential)	
1	51.1473	1	54.161
2	51.1036	2	54.1258
3	51.1523	3	54.1448
4	51.1698	4	54.1594
5	51.1477	5	53.9502
6	51.1254	6	53.9672
7	51.1404	7	54.0906
8	51.1696	8	54.1511
9	51.1588	9	54.0896
10	51.1168	10	54.1403
11	51.1427	11	54.1358
12	51.1508	12	54.1464
13	51.1477	13	54.0562
14	51.1572	14	53.9333
15	51.1484	15	54.0562
16	51.1432	16	54.1911
17	51.1379	17	54.0477
18	51.1491	18	54.1684
19	51.1338	19	54.0492
20	51.0454	20	53.6133
21	51.1785	21	54.1711
22	51.1193	22	54.0799
23	51.1722	23	54.093
24	51.1314	24	54.0812
25	51.1487	25	54.0119
26	51.1287	26	54.1081
27	51.154	27	54.1681
28	51.1614	28	54.1226
29	51.1519	29	54.1519
30	51.1434	30	54.1801
31	51.1406	31	54.1189
32	51.1566	32	54.1727
33	51.1408	33	54.1398
34	51.1136	34	54.1655
35	51.135	35	54.145
36	51.1334	36	54.1461
37	51.1561	37	54.1633
38	51.1495	38	54.0376
39	51.1194	39	54.007
40	51.1507	40	54.1873
41	51.1716	41	53.9998
42	51.1673	42	54.0635
43	51.0609	43	54.1668
44	51.1597	44	54.0147
Average	51.14165	Average	54.09258

Table (3) PSNR by randomly LSB replacement and our proposed in randomly LSB replacement

PSNR (randomly LSB)		PSNR(our proposed randomly LSB)	
1	51.156	1	54.1711
2	51.1407	2	54.0998
3	51.1044	3	54.1697
4	51.1439	4	54.1588
5	51.1329	5	53.9909
6	51.1013	6	53.956
7	51.1765	7	54.1586
8	51.1648	8	54.1533
9	51.1377	9	54.1329
10	51.1218	10	54.1546
11	51.1115	11	54.1602
12	51.1291	12	54.1173
13	51.1495	13	54.0726
14	51.1269	14	53.9707
15	51.1843	15	54.0956
16	51.1742	16	54.1596
17	51.1484	17	54.0749
18	51.1172	18	54.1419
19	51.1449	19	54.006
20	51.1134	20	53.6276
21	51.1225	21	54.1498
22	51.1581	22	54.1016
23	51.1542	23	54.1084
24	51.1516	24	54.0903
25	51.121	25	54.0417
26	51.1686	26	54.1324
27	51.1529	27	54.14
28	51.1265	28	54.1729
29	51.1701	29	54.1748
30	51.1496	30	54.1223
31	51.1536	31	54.1379
32	51.1776	32	54.153
33	51.1055	33	54.135
34	51.1629	34	54.1644
35	51.126	35	54.1652
36	51.1457	36	54.1498
37	51.143	37	54.1226
38	51.1677	38	54.0846
39	51.1586	39	54.0399
40	51.1444	40	54.1938
41	51.1553	41	54.0167
42	51.1442	42	54.0301
43	51.1283	43	54.1588
44	51.1869	44	54.0167
Average	51.14441	Average	54.09943

Table 4 PSNR by LSB Matching replacement and our proposed in LSB Matching replacement. We obtained a higher PSNR rate by 5.78%

PSNR (LSBM)		PSNR (Our proposed LSBM)	
1	51.156	1	54.1711
2	51.1407	2	54.0998
3	51.1044	3	54.1697
4	51.1439	4	54.1588
5	51.1329	5	53.9909
6	51.1013	6	53.956
7	51.1765	7	54.1586
8	51.1648	8	54.1533
9	51.1377	9	54.1329
10	51.1218	10	54.1546
11	51.1115	11	54.1602
12	51.1291	12	54.1173
13	51.1495	13	54.0726
14	51.1269	14	53.9707
15	51.1843	15	54.0956
16	51.1742	16	54.1596
17	51.1484	17	54.0749
18	51.1172	18	54.1419
19	51.1449	19	54.006
20	51.1134	20	53.6276
21	51.1225	21	54.1498
22	51.1581	22	54.1016
23	51.1542	23	54.1084
24	51.1516	24	54.0903
25	51.121	25	54.0417
26	51.1686	26	54.1324
27	51.1529	27	54.14
28	51.1265	28	54.1729
29	51.1701	29	54.1748
30	51.1496	30	54.1223
31	51.1536	31	54.1379
32	51.1776	32	54.153
33	51.1055	33	54.135
34	51.1629	34	54.1644
35	51.126	35	54.1652
36	51.1457	36	54.1498
37	51.143	37	54.1226
38	51.1677	38	54.0846
39	51.1586	39	54.0399
40	51.1444	40	54.1938
41	51.1553	41	54.0167
42	51.1442	42	54.0301
43	51.1283	43	54.1588
44	51.1869	44	54.0167
Average	51.14441	Average	54.09943

The stego-image produced by LSB substitution steganography and the stego-image produced by suggested technique are compared with respect to PSNR parameters in the imperceptibility analysis. Analyzing imperceptibility is used to gauge how much the original image changes as a result of the data-embedding process. The PSNR value of the stego-image should be as high as feasible since a high PSNR value will ensure that the stego-image has superior visual quality. The results show that the PSNR value of the proposed method exceeds their value in the other three methods by a good percentage, proving the effectiveness of the method.

We have compared our scheme with one of the modern steganography schemes, which used LSB replacement, and the images it used from the database SIPI. They suggested a novel n-right most bit replacement image steganography method to embed the secret data in an image, where 1 <= n <= 4. The secret data's n bits and each pixel's n-rightmost bits are transformed to decimal values. In order to create stego-pixels, the original pixels are then readjusted using the difference between these two decimal values (Sahu & Swain, 2019). Which means that when n=1, then one secret bit will be hidden in the first LSB from the right and this is what we have done in our method (1bpp). Because they used the cover image in the size of (512*512) and the secret data (262144 bits) so to compare our method with theirs, we have resized the cover image we used for (512*512) as well as the secret data to (262144 bits). After applying our method on the same images that they used, we made a comparison when they used the first LSB from right at n = 1 because we also used the first LSB from right. The average of PSNR that they obtained at n = 1 was (51.21), while our method obtained an average of PSNR (54.11) at n=1. We obtained higher PSNR rate by 5.85%.

We know that IWT and the use of low frequencies is an existing method. Our contribution is that we have pre-processed the secret image by applying IWT to it before embedding it in the cover image, and its size before pre-processing on it and after pre-processing is of the same size but with higher value of PSNR. With this pre-processing, our secret image remains the same its original size after extraction. And our stego image will be of higher quality.

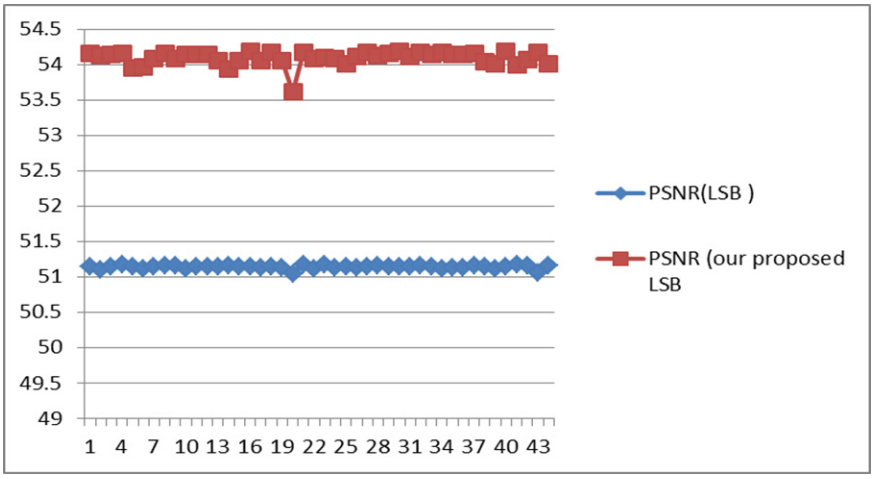

Figure 7. Comparison between PSNR of (LSB sequential) and PSNR of (our proposed LSB sequential)

5 Conclusion

In this paper we have proposed a steganography method based on least significant bit (LSB) replacement and integer wavelet transform IWT through lifting scheme to achieve high quality of stego image. We chose a set of grayscale images from the database SIPI for experiments. We used the dataset as a secret images and pre-processed them using IWT to partition them into several segments and separate the low-frequency segments from the high-frequency segments. As noted in the summary and shown in the results and figures, it is clear that the proposed method is better than the other methods we have compared with it. Suggested method own better PSNR, better picture quality most important of all, attackers cannot easily access confidential data, Thus, we can conclude that the our LSB steganography method is the efficient more suitable scheme for the steganography.

We can suggested study the better result of the Proposed Steganography approach upon adoption of the hybrid transformation (DCT and DWT), and also suggested improving and applying the Proposed steganography method for digital video right protection, and also increasing the level of security of proposed steganography scheme by changing the positions of the secret bits before adding to the host image, as well the proposal to pre-process the cover image by IWT and different mechanism of the embedding process so as to ensure a high quality of the stego image as a future work.

References

A., I. A.-s. (2007). Hiding Data Using LSB-3. J.Basrah Res.

Abdul-Sada, A. I. (2007). Hiding Data Using LSB-3. J.Basrah Res.

Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., & Iliopoulos, C. (2022). Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. alexandria eng. J., 10577-10592.

Aura, T. (1996). Practical Invisibility in Digital Communication. Information Hiding, 266-278.

Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 469-474.

Chen, X., Zou, M., Yang, B., Wang, Z., Wu, N., & Qi, L. (2021). A visually secure image encryption method based on integer wavelet transform and rhombus prediction. Mathematical Biosciences and Engineering/ MBE, 1722–1739.

Gutub, A., & Al-Shaarani, F. (2020). Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. Arab. J. Sci. Eng.

Hempstalk, K. (2006). Hiding Behind corners Using edges in images for better steganography. Multimed. Tools

Appl.

Honeyman, N. P. (2003). Hide and seek: An introduction to steganography. IEEE.

Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. MATIC Web of conference.

Ker, A. D. (2004). Improved Detection of LSB Steganography in Grayscale Images. Lect. Notes Comput. Sci., 97-115.

Maiti, S., Nayak, M. R., & Sarkar, S. K. (2017). Modified Least Significant Bit (LSB) Matching Technique for Robust Information Hiding. J. Emerg. Technol. Innov. Res., 193-200.

Mielikainen, J. (2006). LSB matching revisited. IEEE Signal Process. Lett., 285-287.

Miri, A., & Faez, K. (2018). An image steganography method based on integer wavelet transform," Multimed. Tools Appl., vol. 77, no. 11, pp. Multimed Tools Appl., 13133-13144.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding - a survey. IEEE, 1062-1078.

Pratik , D Shah ; R, S Bichkar. (2018). P. A secure spatial domain image steganography using genetic algorithm and linear congruential generator. Springer Nature Singapore Pte Ltd. 2018. International Conference on Intelligent Computing.

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Secur, 32-44.

S, M., M, R. N., & S, K. S. (2017). Modified Least Significant Bit (LSB) Matching Technique for Robust Information Hiding. J. Emerg. Technol. Innov.

Sahu, A. K., & Swain, G. (2019). A Novel n-Rightmost Bit Replacement Image Steganography Technique. 3DR EXPRESS.

Setiadi, D. I. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimed. Tools Appl.

Shah, P. D., & Bichkar, R. S. (2018). A secure spatial domain image steganography using genetic algorithm and linear congruential generator. International Conference on Intelligent Computing, (pp. 119-129).

Subhedar, M. S., & Mankar, V. H. (2019). Secure image steganography using framelet transform and bidiagonal SVD. Springer Science.

Wang, Y., Tang, M., & Wang, Z. (2020). High-capacity adaptive steganography based on LSB and Hamming code. Optik (Stuttg). .

Weber, A. G. (2018). Ming Hsieh Department of Electrical Engineering USC-SIPI Report # 432 The USC-SIPI Image Database : Version 6 Accessing the Database Images Database on CD-R Media,.

Zhu, L., Song, H., Zhang, X., Yan, M., Zhang, T., Wang, X., & Xu, J. (2020). A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding," Signal Proc107629, 2020, doi: 10.1016/j. sigpro.2020. Signal Processing.