An Improved RDWT-based Image Steganography Scheme with QR Decomposition and Double Entropy

Ke-Huey Ng[1], Siau-Chuin Liew[2], Ferda Ernawan[3]
Faculty of Computing, Universiti Malaysia Pahang
Gambang, Kuantan, Pahang Darul Makmur, Malaysia

***Abstract*—This paper introduces an improved RDWT-based image steganography with QR decomposition and double entropy system. It demonstrates image steganography method that hides grayscale secret image into grayscale cover image using RDWT, QR decomposition and entropy calculation. The proposed scheme made use of the human visual system (HVS) in the embedding process. Both cover and secret image are being segmented into non-overlapping blocks with identical block size. Then, entropy values generated from every image block will be sorted from the lowest value to the highest value. The embedding process starts by embedding the secret image block with lowest entropy value into the cover image block with lowest entropy value. The process goes on until all image blocks have been embedded. Embedding secret image into cover image according to the entropy values causes differences that HVS can less likely to detect because of the small changes on image texture. By applying the double entropy system, proposed scheme managed to achieve a higher PSNR value of 60.3773 while previous work gave a value of 55.5771. In terms of SSIM value, proposed scheme generated a value of 0.9998 comparing to previous work's value of 0.9967. The proposed scheme eliminated the false-positive issue and required low computational time of only 0.72 seconds for embedding and 1.14 seconds for extraction process. Also, it has shown better result compared to previous work in terms of imperceptibility.**

Keywords*—Steganography; image steganography; transform domain; Redundant Discrete Wavelet Transform (RDWT); QR decomposition; entropy; human visual system (HVS); imperceptibility

I. INTRODUCTION

Steganography [1] becomes more and more important as many people joined the cyberspace revolution that involves information exchanging technology. It is the science of information hiding. Its purpose is to convey a message without letting the existence of message being discovered except for the intended receiver, and if being discovered, the message is hard to be detected and recovered. Digital pictures, audio and video are increasingly furnished with distinguishing but imperceptible marks [2], which may contain a hiding copyright serial number or notice. This may directly help to prevent the unauthorized use.

In the context of image steganography, there are two (2) domains which are spatial and transform domain. Spatial domain involves the direct bitwise manipulation whereas transform domain focuses on the transformed image manipulation, which means the original cover image will be changed or transformed first before embedding secret message. Spatial domain is easier to be developed as compared to transform domain. It requires shorter computational time. However, it is more vulnerable to attacks. The reason is that it embeds secret information into cover image directly without transforming the cover image itself, this can cause the secret information to be destroyed easily if the stego image has been attacked.

Thus, transform domain is more preferable because it ensures a certain level of robustness as it withstands against attacks such as geometric attacks and compression. The secret information should still be present and can be detected regardless of the attacks done to stego image. Among different types of transform domain techniques, wavelet transform requires less computational cost compared to DCT and FFT (Fourier Transform) and offers sub-representations of the image that can be considered related to how the human visual system (HVS) perceives images. Generally, the wavelet transform allows embedding data in high frequency regions where the HVS cannot distinguish modifications compared to uniform regions with low frequency.

On the other hand, to avoid unauthorized users attacking stego image easily, the concept of entropy will be applied. It allows the embedding process to be done randomly on image blocks based on the calculation of entropy instead of sequentially placing the secret information from certain pre-set location to another location. This approach enhances the imperceptibility of secret information by embedding the information in image blocks with lower entropy values as they appeared to be less sensitive for HVS. Also, by using this approach, the risk of embedded information being fully attacked or damaged would be lowered because it spreads the secret information randomly on the cover image.

Also, the existing algorithms only do the embedding and extraction process without checking on the extracted information whether it is identical to the original information sent by user. The algorithms are considered not effective because the receiver does not know the trustworthy of information received. There is also a limitation on the embedding capacity of cover image as not every image can be embedded into cover image.

In this paper, an improved RDWT-based image steganography scheme is proposed to enhance the imperceptibility of image. The related work that uses RDWT and matrix factorization techniques will be discussed in Section II. Section III explains the embedding and extraction process of the proposed work. It shows how secret image will

be embedded into cover image by using the double entropy approach. To test the performance of the proposed method, tests for imperceptibility, robustness, false-positive and computational time will be conducted and presented in Section IV. The obtained results will be compared with previous work. Section V concludes this work.

II. Literature Review

A. Frequency Domain Transform Techniques

To be able to achieve good quality and robustness to attacks [2], embedding in transform domain is much more efficient than embedding in spatial domain. The most commonly used frequency-domain transform methods include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Redundant Discrete Wavelet Transform (RDWT). Frequency-domain methods are more widely applied as compared to spatial-domain method.

In information hiding schemes, DFT coefficients gives only modest results and is fragile to attacks, especially sensitive to JPEG and MPEG attacks. Capacity and lack of HVS models are also the drawback of DFT [3] whereas DCT based techniques are robust against simple image processing operations but they are hard to implement, takes more computational time and cost and weak against geometric attacks.

Discrete Wavelet Transform (DWT) is a modern technique popularly utilized in digital image processing. The transforms are based on wavelet of limited duration and different frequency. The wavelet transform decomposes the image into three directions. Most of the image energy concentrates at LL band. Hence, embedding in other sub-bands would lower the quality of image. Hiding information in the transform domain is generally more robust [4, 5] and less perceptible.

As compared to DCT as adopted by Lai [6], DWT has more advantages. As it does not suffer from blocking artefacts, it takes less computational time. Therefore, information hiding techniques based on wavelets are more robust [7] against attacks than those based on DCT.

Comparing DWT and DCT, DWT has better energy compaction and presents a sparse time-frequency but there is a major disadvantage of DWT which is the poor directional selectivity and lack of shift variance.

Redundant Discrete Wavelet Transform (RDWT) is a shift invariance property. Let be the input signal and be its reconstructed version. and are low pass and high pass analysis filters while and are corresponding low pass and high pass synthesis filters and are output coefficients at level j. RDWT avoids down and up sampling of coefficients. During image extraction process, DWT produce inaccuracy [8] because of its shift variances property. Many information hiding schemes apply RDWT to overcome the shirt variance problem [9] of DWT. It removes the down-sampling operation from DWT to produce an over-complete representation [10] of the frequency coefficients. Also, as compared to DWT [11], RDWT is more robust. Besides that, RDWT helps to enhance embedding capacity [12] because its sub-bands have the same size of the original image.

B. Matrix Factorization Techniques

There are several matrix factorization methods such as singular value decomposition (SVD), Schur decomposition, QR decomposition, LU decomposition, etc. [13] resulting from solutions of linear equation.

SVD of an matrix A with dimensions m x m is given by

$$A = USV^T \tag{1}$$

With SVD's good stability, applying it to an image does not cause noticeable change [14, 15] on the appearance.

Schur decomposition of a real matrix A results in two matrices U and D such that

$$A = U \times D \times U' \tag{2}$$

It is suggested to be used in digital image processing [16] as it requires less computational cost than SVD.

QR decomposition or QR factorization [17] is decomposition of matrix into an orthogonal matrix and triangular matrix. Any real matrix A can be expressed as:

$$[Q, R] = qr(A) \tag{3}$$

LU factorization is almost similar to QR decomposition. However, QR decomposition has been proven to be more precise for least square problems. LU factorization [12] can only be applied to square matrices whereas QR factorization can be applied to both square and rectangular matrices.

When comparing SVD with QR decomposition, the latter requires less computational complexity. Another feature of QR decomposition is the resistance to some signal processing operations, such as filtering, lossy compression and noise addition. QR decomposition could also solve the major issue [4] of SVD which is its false positive problem.

C. Arnold Transform

Arnold Transform is widely used in image permutation. It is also called the Cat Face transfer, and it is given by.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \tag{4}$$

Arnold transform is often being applied on involved images to improve the security of information hiding schemes.

D. Image Texture Analysis

There are several ways to measure the texture of a digital image. Entropy is the most suitable way to measure the image's texture content. Texture provides measure of properties of an image such as regularity, coarseness and smoothness. An image that is perfectly flat will have an entropy value of zero. Entropy [18] can be defined as the statistical measure of randomness.

According to Shannon's definition, the entropy of a grayscale image is given by the following mathematical relation:

$$E_1 = -\sum_{i=0}^{L-1} p_i \log p_i \quad (5)$$

If the entropy value is high then it is considered to have more details [19].

E. Performance Evaluation Techniques

To measure the quality of a digital image, PSNR is one of the popular metrics to use. It is done by analyzing the mean squared error value between the Cover and the stego image. The higher the PSNR value [20], the smaller the possibility of visual attack by human eyes. PSNR is being presented as [21].

$$PSNR\ (in\ dB) = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (6)$$

and

$$MSE = \frac{\sum_{i=1}^{N}(C_i - C'_i)^2}{N} \quad (7)$$

On the other hand, SSIM is also used as a metric to measure the similarity between two images. It is being done by.

$$\text{SSIM}\ (x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \quad (8)$$

$$c_1 = (k_1 L)^2 \quad (9)$$

$$c_2 = (k_2 L)^2 \quad (10)$$

The higher the SSIM index is, the better the visual quality [21] of the stego image with respect to the cover image.

F. Related Work

The spatial domain methods are less robust and use simple embedding process. When the issues of imperceptibility and robustness are concerned, the transform domain techniques are a better option [2], especially when they are being tested against geometric attacks.

Recently, many hybrid transform domain methods are being developed to improve the robustness. While individual transform domain techniques such as DFT, DCT and DWT are good enough to improve the properties as mentioned in 2.6, combining them with Singular Value Decomposition (SVD) will further improve the image quality of the scheme. One of the features of SVD is that it helps to achieve good transparency and robustness.

In 2013, Anumol and Anusudha [22] presented a robust scheme based on discrete wavelet transform and singular value decomposition. The paper chose to use DWT over DFT and DCT as the DFT and DCT are full frame transforms and hence any changes in the transform coefficient affects the entire image. In the embedding process, HL and LH sub-bands are used instead of LL and HH band to improve the robustness and imperceptibility. The proposed method is robust against various types of attacks.

In 2016, Mansi and Vijay [12] proposed an image steganography scheme using QR decomposition and RDWT. Artefacts due to variation in energy distribution caused by shifts in input signal have been solved by RDWT. QR decomposition requires less computational complexity and eliminates false positive issue. The proposed work has shown improvement in terms of robustness, capacity and imperceptibility.

In 2016, Taha et al. [15] evaluated the performance of both RDWT-SVD and DWT-SVD schemes. RDWT is a shift invariance property. Many schemes based on RDWT have been proposed to overcome the shift variant problem of DWT. It removes the down-sampling operation from DWT to produce an over-complete representation of the frequency coefficients. Performing SVD on images is computationally costly. By combining SVD with DWT or RDWT, less computational effort is required to produce better performance. Both schemes showed robust against all attacks, RDWT-SVD is better than DWT-SVD, especially for geometrical attacks.

In 2017, Shaoli Jia et al. [4] introduced a scheme based on DWT and QR Decomposition for colour images. The main advantage of using DWT is that it better takes into account the local image characteristics at different resolution levels which can significantly improve the robustness of hidden message. Arnold transform is applied on the message to ensure security. The work used QR decomposition instead because SVD requires greater computational complexity.

In 2018, Poonam et al. [23] presented a scheme for grayscale images based on DWT-SVD. DWT provided better robustness and visible transparency as compared to DCT and DFT. This paper illustrated an improvement in imperceptibility as well as robustness against attacks.

In 2018, Ferda and Muhammad [24] proposed a block-based RDWT-SVD method using human visual system (HVS) characteristics. This scheme presents an embedding method by examining the coefficients in the first column of U vectors. The proposed scheme can avoid the false-positive problem faced by many other RDWT-SVD schemes during extraction process. The hidden image is scrambled by Arnold transform for security purpose. Compared to existing methods, the method achieved better robustness and imperceptibility under various attacks.

In 2018, Divya and [25] developed a false-positive-free scheme based on shuffled SVD (SSVD) and RDWT. The scheme embeds hidden message on the cover image using Redundant Discrete Wavelet Transform (RDWT) and chaotic mapping. Chaotic mapping is achieved by Shuffled singular value decomposition (SSVD). SSVD enhanced the quality of reconstructed image by breaking an image into a set of ensemble images. The proposed work eliminates the false-positive problem that usually found in other RDWT-SVD methods.

Inspired by above-mentioned previous works, an improved image steganography scheme based on RDWT and QR decomposition is proposed to embed grayscale image into grayscale cover image by analyzing the image texture using entropy.

III. Methodologies

This section explains the detailed embedding and extraction process of the proposed work. The proposed scheme made use of the image texture by calculating entropy values for every

image block for both cover and secret images before embedding process (refer to Fig. 1) takes place. Fig. 2 shows the extraction process of proposed method.

The main contribution of the proposed work is the use of entropy in the embedding process. Before embedding takes place, both cover image and secret image will be segmented into non-overlapping blocks with the same block size. Every image block will be computed to produce an entropy value. Then, all values will be sorted in descending order, from the highest entropy value to the lowest entropy value. This applies to both cover and secret image.

Starting from the block with the highest entropy value, RDWT will be applied on the blocks. The LL sub-band of cover image block will then be decomposed by QR decomposition. The secret image information is embedded by modifying the R value of the LL sub-band of cover image. After that, inverse QR decomposition is performed to get the modified LL sub-band. Them, inverse RDWT will be applied to get the modified image block. This process will continue until all secret image information is being embedded. Finally, a stego image will be formed by combining all modified image blocks.

The reason to use RDWT instead of other transform techniques is that, RDWT removes the coefficients' up-sampling and down-sampling that exists in DWT. Also, RDWT can increase robustness and provides more embedding capacity. On the other hand, QR decomposition provides better imperceptibility and avoids false positive issue, as compared to SVD.

Entropy identifies the texture of a digital image. The higher the entropy value of an image block, the more details it contains. By utilizing the use of entropy during embedding process, the cover image block with the highest entropy value will be embedded with the secret image block with the highest entropy value. The minor changes in the particular image block will not cause significant effect on the entropy values. Now, imagine the secret image block with the highest entropy value, which contains more details, is embedded into the cover image block with the lowest entropy. This process will cause more changes in the image texture as compared to the previous case, which will indirectly affect the imperceptibility of the scheme.

The proposed work embeds secret image into cover image by following the steps shown in Fig. 1. By considering the order of entropy values of all image blocks, higher imperceptibility is achieved. As the image block with highest entropy value will remain having the highest entropy value as it is embedded with another image block, which, in this case, the secret image block with the highest entropy value. This will not be accomplished if the process replaces any of the image block with entropy value of different order instead of the same order because the image texture will be changed in a different manner that causes more differences.

Fig. 2 demonstrates the extraction process which extracts secret image information from the image location that was set during the embedding process. There is no need for re-calculation of entropy values for every image blocks.

A. Embedding Process

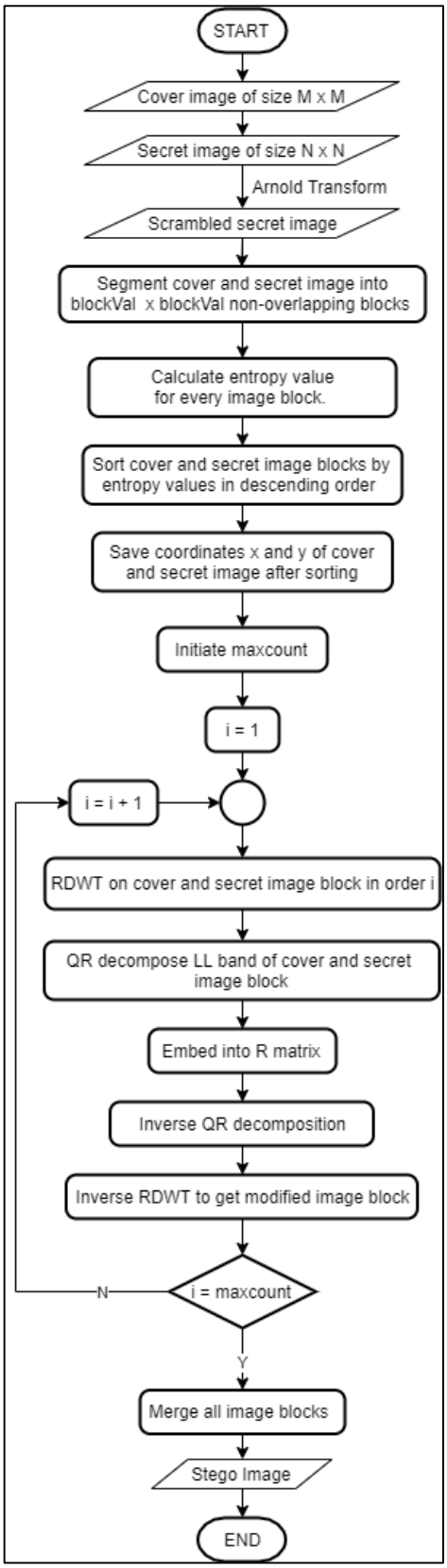


Fig. 1. Embedding Process of Proposed Method.

The embedding algorithm:

Input: Cover Image; Secret Image

Pre-processing:

Step 1: Segment cover image, c of size M x M into blocksize x blocksize non-overlapping blocks.
Step 2: Apply Arnold transform on secret image.

$$\mathbf{S'} = \mathbf{arnold}(\mathbf{S}, \mathbf{key}) \quad (11)$$

Step 3: Segment secret image, s of size N x N into blocksize x blocksize non-overlapping blocks.
Step 4: Calculate entropy for each cover image blocks.
Step 5: Sort the cover image blocks according to entropy values from highest to lowest.
Step 6: Save coordinates of x_c and y_c after sorting.
Step 7: Calculate entropy for each secret image blocks.
Step 8: Sort the secret image blocks according to entropy values from highest to lowest.
Step 9: Save coordinates of x_s and y_s after sorting.

Secret Image Embedding:

Step 10: Select cover image blocks from the highest entropy value to the lowest.
Step 11: Each selected blocksize x blocksize cover image block is transformed by 1-level RDWT.

$$\left[\mathbf{LL}_{\boldsymbol{c}}, \mathbf{LH}_{\boldsymbol{c}}, \mathbf{HL}_{\boldsymbol{c}}, \mathbf{HH}_{\boldsymbol{c}}\right] = \mathbf{rdwt}(\mathbf{cover\ image\ block}) \quad (12)$$

Step 12: Select secret image blocks from the highest entropy value to the lowest.
Step 13: Each selected blocksize x blocksize secret image block is transformed by 1-level RDWT.

$$\left[\mathbf{LL}_{\boldsymbol{s}}, \mathbf{LH}_{\boldsymbol{s}}, \mathbf{HL}_{\boldsymbol{s}}, \mathbf{HH}_{\boldsymbol{s}}\right] = \mathbf{rdwt}(\mathbf{secret\ image\ block}) \quad (13)$$

Step 14: The LL subband of cover image block is decomposed by QR decomposition.

$$\left[\boldsymbol{Q}_{\boldsymbol{c}}, \boldsymbol{R}_{\boldsymbol{c}}\right] = \mathbf{qr}(\mathbf{LL}_{\boldsymbol{c}}) \quad (14)$$

Step 15: The LL subband of secret image block is decomposed by QR decomposition.

$$\left[\boldsymbol{Q}_{\boldsymbol{s}}, \boldsymbol{R}_{\boldsymbol{s}}\right] = \mathbf{qr}(\mathbf{LL}_{\boldsymbol{s}}) \quad (15)$$

Step 16: The secret image is embedded by modifying the R value of the LL_c.

$$\boldsymbol{R}_{\boldsymbol{st}} = \boldsymbol{R}_{\boldsymbol{c}} + \propto \boldsymbol{R}_{\boldsymbol{s}} \quad (16)$$

Step 17: Perform inverse QR decomposition to get the modified LL_c to form LL_{st}.

$$\mathbf{LL}_{\boldsymbol{st}} = \boldsymbol{Q}_{\boldsymbol{c}} \times \boldsymbol{R}_{\boldsymbol{st}} \quad (17)$$

Step 18: Apply inverse RDWT to get the modified image block

$$\mathbf{Modified\ image\ block} = \boldsymbol{RDWT}^{-1}\left(\mathbf{LL}_{\boldsymbol{st}}, \mathbf{LH}_{\boldsymbol{c}}, \mathbf{HL}_{\boldsymbol{c}}, \mathbf{HH}_{\boldsymbol{c}}\right) \quad (18)$$

Step 19: Repeat step 10-18 until all secret image blocks have been embedded.

Post-processing:

Step 20: Merge all modified image blocks to form Stego Image.

Output: Stego Image

B. Extraction Process

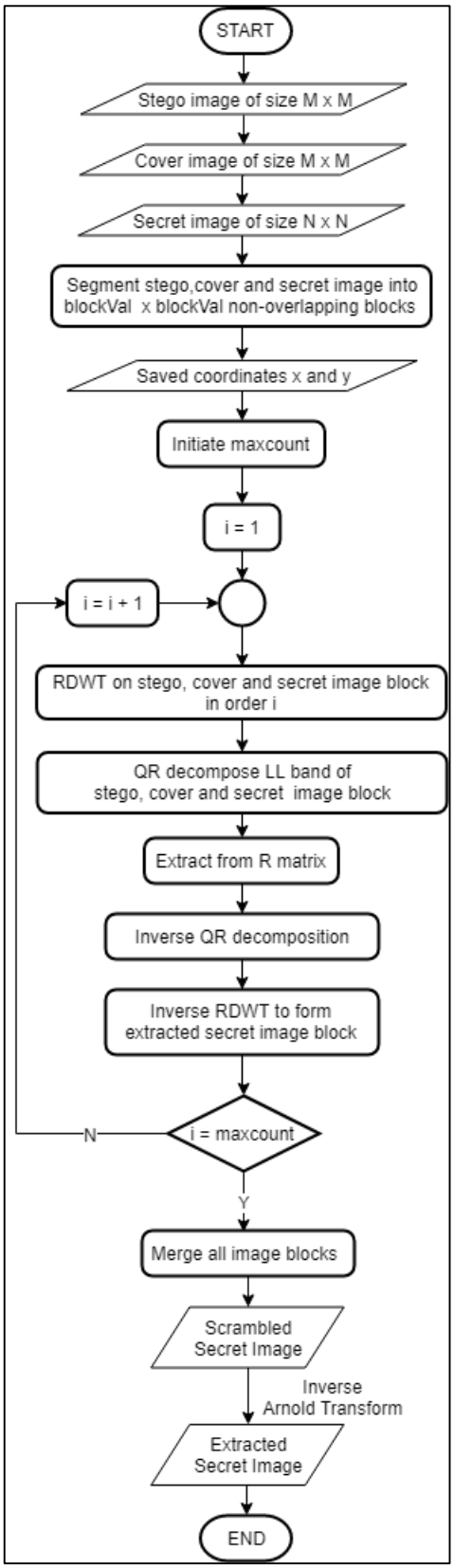


Fig. 2. Extraction Process of Proposed Method.

The extraction algorithm:

Input: Stego Image; Cover Image; Secret Image

Pre-processing:

Step 1: Segment stego image , st of size M x M into blocksize x blocksize non-overlapping blocks.
Step 2: Segment cover image, c of size M x M into blocksize x blocksize non-overlapping blocks.
Step 3: Segment secret image, s of size N x N into blocksize x blocksize non-overlapping blocks.

Secret Image Extraction:

Step 4: Select stego image blocks from the highest entropy value to the lowest according to
the x_c and y_c coordinates obtained.
Step 5: Each selected blocksize x blocksize stego image block is transformed by 1-level RDWT.

$$[\mathbf{LL}_{st}, \mathbf{LH}_{st}, \mathbf{HL}_{st,}\mathbf{HH}_{st}] = \mathbf{rdwt}(\mathbf{stego\ image\ block}) \quad (19)$$

Step 6: Select cover image blocks from the highest entropy value to the lowest according to
the x_c and y_c coordinates obtained.
Step 7: Each selected blocksize x blocksize cover image block is transformed by 1-level RDWT.

$$[\mathbf{LL}_{c}, \mathbf{LH}_{c}, \mathbf{HL}_{c,}\mathbf{HH}_{c}] = \mathbf{rdwt}(\mathbf{cover\ image\ block}) \quad (20)$$

Step 8: Select secret image blocks from the highest entropy value to the lowest according to
the x_s and y_s coordinates obtained.
Step 9: Each selected blocksize x blocksize secret image block is transformed by 1-level RDWT.

$$[\mathbf{LL}_{s}, \mathbf{LH}_{s}, \mathbf{HL}_{s,}\mathbf{HH}_{s}] = \mathbf{rdwt}(\mathbf{secret\ image\ block}) \quad (21)$$

Step 10: The LL subband of stego image block is decomposed by QR decomposition.

$$[\boldsymbol{Q}_{st,}, \boldsymbol{R}_{st}] = \mathbf{qr}(\mathbf{LL}_{st}) \quad (22)$$

Step 11: The LL subband of cover image block is decomposed by QR decomposition.

$$[\boldsymbol{Q}_{c,}, \boldsymbol{R}_{c}] = \mathbf{qr}(\mathbf{LL}_{c}) \quad (23)$$

Step 12: The LL subband of secret image block is decomposed by QR decomposition.

$$[\boldsymbol{Q}_{s,}, \boldsymbol{R}_{s}] = \mathbf{qr}(\mathbf{LL}_{s}) \quad (24)$$

Step 13: The secret image is extracted by

$$\boldsymbol{R}_{s2} = (\boldsymbol{R}_{st} - \boldsymbol{R}_{c}) / \propto \quad (25)$$

Step 14: Perform inverse QR decomposition to form LL_{s2}.

$$\mathbf{LL}_{s2} = \boldsymbol{Q}_{s} \times \boldsymbol{R}_{s2} \quad (26)$$

Step 15: Apply inverse RDWT to get the extracted secret image block.

$$\mathbf{Extracted\ secret\ image\ block} = \boldsymbol{RDWT}^{-1}(\mathbf{LL}_{s2}, \mathbf{LH}_{s}, \mathbf{HL}_{s,}\mathbf{HH}_{s}) \quad (27)$$

Step 16: Repeat step 4-15 until all secret image blocks have been extracted.

Post-processing:

Step 17: Merge all extracted image blocks to form image S2.
Step 18: Apply inverse Arnold transform on image S2 to get secret image S_{ext}.

$$\boldsymbol{S}_{ext} = \mathbf{inarnold}(\mathbf{S2}, \mathbf{key}) \quad (28)$$

Output: Extracted Secret Image

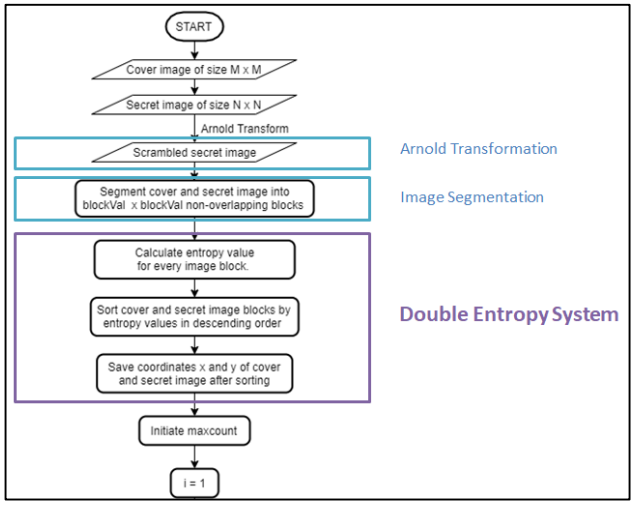


Fig. 3. Part of Embedding Process.

C. Double Entropy System

The double entropy system is what differentiates this proposed scheme from other steganography schemes. It happens right before embedding process takes place as shown in Fig. 3.

The double entropy system considers both entropy values of cover image blocks and secret images blocks before embedding process begins. By making use of the human visual system, cover and secret image have been segmented into blocks of equal size and each image block has an entropy value. All entropy values are then being sorted in descending order.

When embedding process starts, secret image block with the highest entropy value will be embedded into the cover image block with the highest entropy value. The embedding process continues until all secret image blocks have been embedded into cover image according to their corresponding entropy values, from the highest value to the lowest value.

By initiating embedding process according to the entropy values of both cover and secret image blocks, the block that higher entropy value, hence, more details will be embedded into another block that has more details. Through this process, the cover image block that originally has the high level of detail will remained as it is but it now contains the secret image information. The block remains having high entropy values and has least impact on human visual system as it is harder to notice the difference before and after embedding as compared to block with lower entropy value. Proposed work utilizes the double entropy system that applies entropy calculation on both

cover and secret image in order to find out the areas that are more suitable for embedding to achieve a better-quality stego image. When there are changes or modification happens in that particular area, HVS will less likely to notice the difference because of its low sensitivity towards the area. It is to believe that the imperceptibility of proposed scheme will be improved through this approach.

IV. Results and Discussion

To demonstrate the effect of different aspects of proposed scheme, different experiments have been carried out including the imperceptibility test, false positive test and computational time evaluation.

The images used in these experiments are lena, baboon, peppers, lake, house, jetplane, livingroom, pirate, bridge, boat, cameraman and barbara as demonstrated in Table IX. The cover image size is set to be 512x512. The sizes of secret image are of 32x32, 64x64, 128x128, 256x256 and 512x512 in order to compare how image size affects the imperceptibility of stego image.

A. Imperceptibility Test

The proposed work consists of three techniques, which include RDWT, QR decomposition and double entropy. To show how adding double entropy into the scheme helps with achieving better imperceptibility, two different experiments have been carried out. There will be one experiment using double entropy in the embedding process and the other one will eliminate double entropy during the embedding process.

Every experiment uses different combination of cover image and secret image to generate PSNR and SSIM values. In order to achieve a fair comparison of imperceptibility, the cover and secret images used in proposed scheme will be the same as the work being compared with. The experiments will be carried out by varying the size of segmented block and the size of secret image in order to show how they affect the imperceptibility of the scheme.

The average PSNR and SSIM values for each experiment are presented in Table I, Table II, Table III, Table IV and Table V. The average PSNR values of all experiments are being presented in Table VI.

From the results above, t is shown that proposed work that uses RDWT, QR decomposition and double entropy has the highest PSNR value compared to the other two experiments. On the other hand, the experiment that uses RDWT and QR decomposition without including double entropy gives the second highest PSNR value while the one that uses only RDWT and double entropy without QR decomposition generates the lowest PSNR value.

By analysing on the average PSNR values for different secret image sizes, it is believed that the smaller the secret image size, the higher the PSNR value. This is because of the smaller amount of information being embedded into cover image, hence, smaller modification made on the cover image.

In order to achieve a fair comparison of imperceptibility between proposed scheme and existing work, the cover and secret images used will be the same as the work being compared with.

From the comparison of PSNR and SSIM values presented in Table VII and Table VIII, it is shown that proposed scheme performed better in terms of imperceptibility as compared to existing work due to the utilization of double entropy system in embedding process.

TABLE. I. Average PSNR (without Double Entropy)

Secret Image Size	Block Size			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	74.9414	74.8407	74.7871	-
64 x 64	68.5213	68.5471	68.5892	68.6398
128 x 128	62.3082	62.3500	62.4002	62.7121
256 x 256	56.1674	56.2770	56.2964	56.3785
512 x 512	50.1361	50.1827	50.2526	50.3078

TABLE. II. Average SSIM (without Double Entropy)

Secret Image Size	Block Size			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	0.9999	1.0000	1.0000	-
64 x 64	0.9997	0.9998	0.9999	0.9999
128 x 128	0.9991	0.9994	0.9996	1.0830
256 x 256	0.9976	0.9985	0.9989	0.9991
512 x 512	0.9977	0.9983	0.9985	0.9921

TABLE. III. Average PSNR (with Double Entropy)

Secret Image Size	Block Size			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	74.9260	74.9106	74.9695	-
64 x 64	68.5912	68.6517	68.6974	68.8272
128 x 128	62.3726	62.4577	62.5343	62.6374
256 x 256	56.2711	56.3604	56.4219	56.4909
512 x 512	50.1862	50.2788	50.3361	50.3986

TABLE. IV. Average SSIM (with Double Entropy)

Secret Image Size	Block Size			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	1.0000	1.0000	1.0000	-
64 x 64	0.9999	1.0000	1.0000	1.0000
128 x 128	0.9999	0.9999	0.9998	0.9998
256 x 256	0.9997	0.9996	0.9995	0.9995
512 x 512	0.9991	0.9989	0.9987	0.9985

TABLE. V. AVERAGE PSNR (WITHOUT QR DECOMPOSITION)

Secret Image Size	Block Size			
	4 x 4	8 x 8	16 x 16	32 x 32
32 x 32	74.8736	74.7302	74.6736	-
64 x 64	68.5102	68.4552	68.4295	68.4037
128 x 128	62.2878	62.2651	62.2560	62.2435
256 x 256	56.1576	56.1444	56.1386	56.1312
512 x 512	50.0773	50.0644	50.0609	50.0575

TABLE. VI. AVERAGE PSNR VALUES BETWEEN 3 EXPERIMENTS

Secret Image Size	Experiments		
	Without Double Entropy	With Double Entropy	Without QR Decomposition
32 x 32	74.8564	**74.9354**	74.7591
64 x 64	68.5744	**68.6919**	68.4497
128 x 128	62.4426	**62.5005**	62.2631
256 x 256	56.2798	**56.3861**	56.1430
512 x 512	50.2198	**50.2999**	50.0650

TABLE. VII. COMPARISON OF IMPERCEPTIBILITY WITH DIVYA AND RANJAN'S WORK BY PSNR VALUES

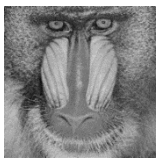
Secret Images	Cover Image	Divya and Ranjan's	Proposed
 and 的		54.3157	60.3666
		54.0472	60.3674
		58.3684	60.3980

TABLE. VIII. COMPARISON OF IMPERCEPTIBILITY WITH FERDA'S WORK BY SSIM VALUES

Secret Image	Cover Image	Ferda's	Proposed
福		 SSIM = 0.9965	 SSIM = **0.9999**
福		 SSIM = 0.9968	 SSIM = **0.9998**

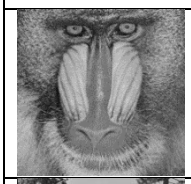
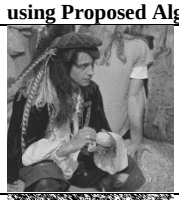
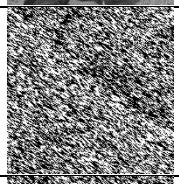
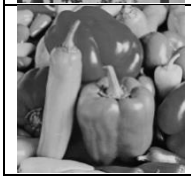
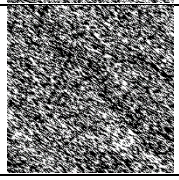
B. *False Positive Test*

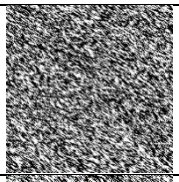
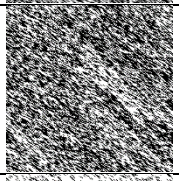
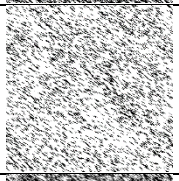
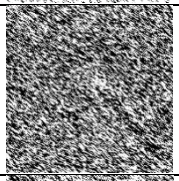
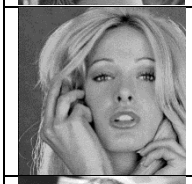
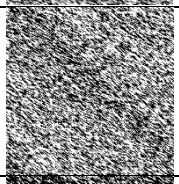
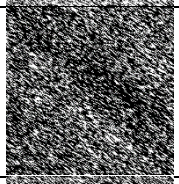
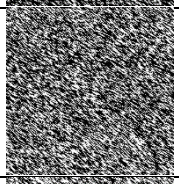
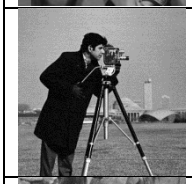
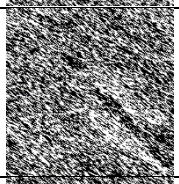
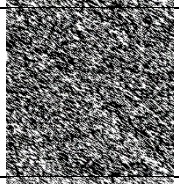
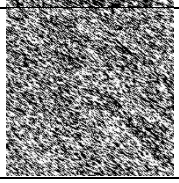
A false positive issue occurs when the image extracted from an unauthorized or arbitrary image shows a visual trace of the owner's original embedded image. This test is conducted using the proposed RDWT-QR scheme with double entropy system. The original embedding and extraction process are done by using Baboon as the cover image and Pirate as the embedded secret image.

Table IX shows the extracted images and respective NC values using the original stego image (Baboon) and other test images.

From the results shown in Table IX, it showed that proposed work can extract secret image from the correct stego image with high NC value (i.e. 0.8889). By changing the stego image to 12 other test images, the extracted image is meaningless and does not ensemble the original embedded secret image. The NC values obtained is very low, ranging from -0.0066 to 0.0127. Therefore, it is proved that the false positive issue that normally occurred in other steganography schemes can be avoided by using proposed algorithm.

TABLE. IX. FALSE POSITIVE TEST RESULTS FOR PROPOSED METHOD

Test Image(s)	Extracted Secret Image using Proposed Algorithm	NC Values
		0.8889
		-0.0065
		0.0094

		0.0026
		-0.0033
		0.0108
		-0.0112
		0.0085
		0.0091
		-0.0066
		0.0127
		0.0110
		-0.0008

C. Computational Time

Table X shows the total embedding time for secret image of different sizes with varying block size whereas Table XI presents the total extraction time for secret image of different sizes with varying block size.

The time taken to embed secret image is slightly longer than the extraction process as shown in the comparison presented in Table XII. The reason is that the embedding of secret image takes more time during the selection of position to embed after calculating entropy values for each segmented image block. This process has been shortened during the extraction process as the position to extract secret information has already been set because of the saved coordinates of x and y.

Table XIII shows that proposed work spent less computational time on embedding process than Ferda's [24] and Divya and Ranjan's [25] work. For the extraction process, proposed work spent a slightly longer time compared to Divya and Ranjan's and 24 seconds faster than Ferda's. Due to the lower complexity of the algorithm, the time taken to execute the embedding and extraction process is shorter.

TABLE. X. EMBEDDING TIME FOR VARYING SECRET IMAGE SIZE WITH DIFFERENT BLOCK SIZE (IN SECONDS)

Secret Image Size	**Block Size**			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	0.78	0.34	1.11	-
64 x 64	3.59	0.69	1.22	0.30
128 x 128	9.33	3.84	1.66	0.50
256 x 256	20.80	9.83	4.61	1.23
512 x 512	61.72	24.52	10.38	5.02

TABLE. XI. EXTRACTION TIME FOR VARYING SECRET IMAGE SIZE WITH DIFFERENT BLOCK SIZE (IN SECONDS)

Secret Image Size	**Block Size**			
	4 x 4	**8 x 8**	**16 x 16**	**32 x 32**
32 x 32	0.67	0.14	0.08	-
64 x 64	3.61	0.80	0.19	0.16
128 x 128	7.42	3.70	1.47	0.38
256 x 256	19.05	8.08	4.17	1.15
512 x 512	60.32	22.74	8.83	4.81

TABLE. XII. AVERAGE COMPUTATION TIME FOR PROPOSED WORK (IN SECONDS)

Secret Image Size	**Embedding**	**Extraction**
32 x 32	0.74	0.30
64 x 64	1.45	1.19
128 x 128	3.83	3.24
256 x 256	9.12	8.11
512 x 512	25.41	24.18

TABLE. XIII. COMPARISON OF COMPUTATION TIME

Embedding (in seconds)			**Extraction (in seconds)**		
Ferda's	**Ranjan's**	**Proposed**	**Ferda's**	**Ranjan's**	**Proposed**
86.2969	0.79	**0.72**	25.3125	**0.22**	1.14

V. CONCLUSION

To test the effectiveness of the proposed scheme, several tests have been conducted. These include the imperceptibility test, false-positive test and computational time taken for both embedding and extraction process.

Test results have shown that proposed scheme has higher imperceptibility and provides image with better quality as compared to previous work by applying the double entropy system.

In terms of computational time and cost, the time taken to embed secret image into cover image and the time taken to extract secret image from stego image are way faster than compared work. Due to the less complex execution of the proposed algorithm, it has reduced the time taken to complete both embedding and extraction process.

On the other hand, the proposed scheme provides a certain level of security by applying Arnold transform on secret image before embedding. It also eliminates the occurrence of false-positive errors, which has been found in many other existing works. Furthermore, RDWT allows embedding of the same-sized secret image into cover image as compared to DWT that only offers half the embedding capacity of RDWT. It also solves the shirt variance problem that caused by DWT to avoid inaccuracy during extraction process.

As a conclusion, the comparison results have shown that proposed work enhanced the imperceptibility of the scheme and eliminates the false-positive issue. Also, proposed work took shorter time to execute embedding and extraction process.

ACKNOWLEDGMENT

The authors sincerely thank Universiti Malaysia Pahang, Malaysia, for providing financial support for this work through UMP Postgraduate Research Grants Scheme (RDU1703280).

REFERENCES

[1] Thiyagarajan, P.; Aghila, G.; Prasanna, Venkatesan V., "Stego-Image Generator (SIG) – Building Steganography Image Database," CDBR-SSE Lab Department of Computer Science, Pondicherry University, Puducherry 605014, 2012.

[2] Prerna Gupta, Girish Parmar, "Image Watermarking using IWT-SVD and its Comparative Analysis with DWT-SVD," in International Conference on Computer, Communications and Electronics (Comptelix), 2017.

[3] Serdean C.V., Tomlinson M., Wade G.J., Ambroze A.M., "Protecting intellectual rights: Digital watermaking in the wavelet domain," in Trends and Recent Achievements in Information Technology, 2002. K. Elissa, “Title of paper if known,” unpublished.

[4] Shaoli Jia, Qingpo Zhou and Hong Zhou, "A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition," Journal of Applied Science and Engineering, pp. 193-200, 2017.

[5] L.-Y. Hsu, H.-T. Hu, "Robust blind image watermarking using crisscross inter-block prediction in the DCT domain," J. Vis. Commun. Image R., pp. 33-47, 2017.

[6] Lai, C.C, "An improved SVD-based watermarking scheme using human visual," Optical Commununication, pp. 938-944, 2011.

[7] Serdean C.V., Tomlinson M., Wade G.J., Ambroze A.M., "Protecting intellectual rights: Digital watermaking in the wavelet domain," in Trends and Recent Achievements in Information Technology, 2002.

[8] Bradley, A.P., "Shift-invariance in the discrete wavelet transform," in Proc. VIIth Digital Image Computing: Techniques and Applications, 2003.

[9] Hien T.D., Nakao Z., Chen Y.W., "RDWT domain watermarking based on independent component analysis extraction," Advance Software Computing, pp. 401-414, 2006.

[10] Nasrin M. Makbol, Bee Ee Khoo, Taha H. Rassem, "Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics," IET Image Process, pp. 34-52, 2016.

[11] F. JE., "The redundant discrete wavelet transform and additive noise," Signal Processing Letters, pp. 629-632, 2005.

[12] M.S. Subhedar, V.H. Mankar, "Image steganography using redundant discrete wavelet transform and QR factorization," Computers and Electrical Engineering, pp. 406-422, 2016.

[13] Q. Su et al., "Embedding color watermarks in color images based on Schur decomposition," Optics Communications 285, pp. 1792-1802, 2012.

[14] Sunil et al., "An Improved Image Steganography based on 2-DWT-FFT-SVD on YCBCR Color Space," in International Conference on Trends in Electronics and Informatics, 2017.

[15] Taha H. Rassem, Nasrin M. Makbol, and Bee Ee Khoo, "Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes," in International Conference on Advanced Science, Engineering and Technology (ICASET), 2016.

[16] G.H. Golub, C.F. Van Loan, "Matrix Computations," Johns Hopkins University Press, Baltimore, 1989.

[17] C.-J. Ahn, "Ahn CJ . Parallel detection algorithm using multiple QR decompositions with permuted channel matrix for SDM/OFDM.," IEEE Transactions on Vehicular Technology, pp. 2578-2582, 2008.

[18] Manoj Kumar, Gursewak Singh, "Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach," International Journal of Computer Applications (0975 – 8887), 2017.

[19] Swati Bhargava and Manish Mukhija, "Hide Image and Text Using LSB, DWT and RSA Based on Image Steganography," ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, pp. 1940-1946, 2019.

[20] Hossain et al., "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation," in Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009), Dhaka, Bangladesh, 2009.

[21] I.J. Kadhim, P. Premaratne and P.J. Vial et al., "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, pp. 299-326, 2019.

[22] Anumol Joseph, K. Anusudha, "Robust watermarking based on DWT SVD," International Journal of Signal & Image Processing, 2013.

[23] Poonam, Shaifali M.Arora, "A DWT-SVD based Robust Digital Watermarking for Digital Images," in International Conference on Computational Intelligence and Data Science (ICCIDS), 2018.

[24] F. Ernawan, M. N. Kabir, "A block-based RDWT-SVD image watermarkingmethod using human visual system characteristics," The Visual Computer, 2018.

[25] J L Divya Shivani, Ranjan K. Senapati, "False-positive-free, Robust and Blind Watermarking Scheme based on Shuffled SVD and RDWT," Journal of Advanced Research in Dynamical and Control Systems, 2018