Future Computing and Informatics Journal

Volume 6
Issue 2 (2021) *Issue 2*

Article 2

2021

Image Hiding Using QR Factorization And Discrete Wavelet Transform Techniques

Reham Ahmed El-Shahed
Ain Shams university, rehamahmed@cis.asu.edu.eg

Maryam Al-Berry
maryam_nabil@cis.asu.edu.eg

Hala Ebied
halam@cis.asu.edu.eg

Howida Shedeed
dr_howida@cis.asu.edu.eg

Future Computing and Informatics Journal

Volume 6
Issue 2 (2021) *Issue 2*

Article 2

2021

Image Hiding Using QR Factorization And Discrete Wavelet Transform Techniques

Reham Ahmed El-Shahed
Ain Shams university, rehamahmed@cis.asu.edu.eg

Maryam Al-Berry
maryam_nabil@cis.asu.edu.eg

Hala Ebied
halam@cis.asu.edu.eg

Howida Shedeed
dr_howida@cis.asu.edu.eg

Future Computing and Informatics Journal

Homepage: https://digitalcommons.aaru.edu.jo/fcij/

doi: http://Doi.org/10.54623/fue.fcij.6.2.2

Image Hiding Using QR Factorization And Discrete Wavelet Transform Techniques

Reham Ahmed El-Shahed[1,a], Maryam Al-Berry[1,b], Hala Ebied[1,c], Howida A. Shedeed[1,d]

[1] Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

[a] rehamahmed@cis.asu.edu.eg, [b] maryam_nabil@cis.asu.edu.eg, [c] halam@cis.asu.edu.eg
[d] dr_howida@cis.asu.edu.eg

ABSTRACT

Steganography is one of the most important tools in the data security field as there is a huge amount of data transferred each moment over the internet. Hiding secret messages in an image has been widely used because the images are mostly used in social media applications. The proposed algorithm is a simple algorithm for hiding an image in another image. The proposed technique uses QR factorization to conceal the secret image. The technique successfully hid a gray and color image in another one and the performance of the algorithm was measured by PSNR, SSIM and NCC. The PSNR for the cover image was in the range of 41 to 51 dB. DWT was added to increase the security of the method and this enhanced technique increased the cover PSNR to 48 t0 56 dB. The SSIM is 100% and the NCC is 1 for both implementations. Which improves that the imperceptibility of the algorithm is very high. The comparative analysis showed that the performance of the algorithm is better than other state-of-the-art algorithms.

KEYWORDS

Image Hiding, Steganography, QR factorization, LU factorization, Discrete Wavelet Transform

https://digitalcommons.aaru.edu.jo/fcij/vol6/iss2/2
DOI: http://doi.org/10.54623/fue.fcij.6.2.2

1. INTRODUCTION

Nowadays, digital steganography has become an important tool for hiding digital data and keep it secured during transmission. Steganography applications are used for medical, military and financial purposes. Steganography is defined as the art of hiding or concealing. There are three main components in digital steganography system, the secret object, the cover object and the hiding algorithm. The secret object is the secret message that needs to be secured. The cover object is the carrier for the secret data where the secret data is embedded. Last, the hiding algorithm is the procedure or technique applied to conceal the secret object in the cover object and this phase results in a stego-object [1].

Both the secret and the cover objects in digital steganography system can be of different types such as binary data, text, image, audio or video.

Images are widely used in social media applications Facebook, Instagram, Pinterest, … etc. Secret data can be embedded in an image file and this is called image steganography.

Image steganography techniques are evaluated by different metrics. The first one is the hiding capacity which means the maximum amount of secret data that can be embedded in the cover object. The second metric is the visual quality or the similarity between the original cover image and the produced stego-image. "Security" is the third metric, it means the resistance of the stego-image against different attacks [2].

There are two types of image steganography methods, spatial-domain methods and transform-domain methods. The spatial-domain methods are directly deal with the image pixels to conceal the secret data, while in the transform-domain methods the cover image is firstly converted to another form before embedding the secret data [2].

The main advantages of the spatial-domain methods that they are simple in implementation, deal with pixels directly, take less computational time and achieve high hiding capacity and high visual quality.

The main problems for spatial-domain methods are high detectability and vulnerability against geometric attacks.

Transform-domain methods are complex, deal with the transformed coefficients of the image, have limited hiding-capacity but they are more robust against attacks [2].

There are different techniques for hiding in image in the spatial-domain, Least Significant Bit (LSB) methods [3], Pixel Value Difference (PVD) based methods[4], Exploiting Modification Direction (EMD) based method [5], Multi-Base Notation System (MBNS) based methods [6], Pixel Pair Matching (PPM) based methods [7], Gray Level Modification (GLM) based methods [8], Pixel Value Prediction (PVP) based methods [9], histogram-based methods [10], edge-based methods [11], mapping-based methods [12] and color model-based methods[13].

Recent steganography algorithms also used different types of matrix decomposition

Published by Arab Journals Platform, 2021

to enhance the robustness of the steganography algorithms. There are different types of matrix decomposition techniques, such as Singular Value Decomposition (SVD), QR factorization, Lower-Upper (LU) factorization, and Schur decomposition. These techniques are used along with transform-domain techniques to enhance the algorithm.

In this paper, a new image steganography algorithm is suggested. The algorithm has been implemented in two ways. First, an algorithm was implemented which depends on QR factorization to hide a grayscale image in a color image. Then, the same algorithm was implemented using QR factorization and Discrete Wavelet Transform (DWT).

The rest of the paper is organized as follows; section 2 is a review of some image steganography techniques. Section 3- presents the proposed method and algorithms in detail. Section 4, contains the performance criteria and results. Section 5- concludes the paper.

2. RELATED WORK

This is a review section for some recent image steganography algorithms.

Kamaldeep et al. [14] proposed a method of image hiding, which hid the information in a selected pixel and on the next value of the selected pixel. A mathematical function was applied on the 7th bit of the pixels, that generated a temporary variable (pixel + 1). The 7th bit of the selected pixel and the 7th bit of pixel + 1 were used for hiding and extracting information. The performance of the method was checked using PSNR and MSE and then compared to other proposed techniques. This proposed image steganography showed interesting, promising results when compared to other existing techniques.

In [15] another image steganography algorithm was proposed. The proposed algorithm used the Most Significant Bit (MSB) of randomly selected pixels to increase the capacity and the security of the hidden data. Two phases are performed to hide the secret message. In the first phase, the channels for hiding were decided. In the second phase, the number of bits to be hidden was decided. The performance of the method was measured by the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM). The results showed that the proposed method has achieved the highest capacity among all existing methods without any distortion in the image.

Firas A. Jassim [16] proposed a steganography algorithm for hiding a text message in an image. The secret message was hidden inside the cover image using Five Modulus Method. The model consists of transforming all the pixels within the 5×5 window size into its corresponding multiples of 5. Then, the secret message is hidden inside the 5×5 window as a non-multiples of 5. As the modulus of non-multiples of 5 are 1,2,3 and 4, therefore; if the reminder is one of these, then this pixel represents a secret character. The advantage of this algorithm was to keep the size of the cover image constant while the secret message increased in size. PSNR was measured for each of the images tested. Based on the PSNR value of each image, the stego-image has a high PSNR value. This new steganography

https://digitalcommons.aaru.edu.jo/fcij/vol6/iss2/2
DOI: http://doi.org/10.54623/fue.fcij.6.2.2

algorithm was very efficient to hide the data inside the image.

As the LSB is the most popular technique in image steganography, Ahmed and Ahmed [17] proposed an LSB-based image steganography algorithm. The algorithm proposed two layers of encryption and hiding stages. First, the message was encrypted by using a secret key that was extracted from MSB and double XOR operations using binary representation. Then, an encrypted stream of bits was hidden into the cover image using the LSB technique. The quality of the proposed method was measured by Mean Square Error (MSE), PSNR, Entropy and histogram distribution. The experimental results showed that the proposed method had acceptable results and it preserves the security of hidden text messages. The results achieved for PSNR and MSE are 55.67 dB and 0.18 respectively.

An LU Factorization-based technique was proposed in [18]. The proposed technique successfully hid an image in another image. The technique depends on the LU decomposition technique to hide the secret image. The performance of the algorithm was measured using PSNR, SSIM and Normalized Cross Correlation (NCC). The PSNR of the cover image was ranging from 36 to 44 dB. The SSIM between secret and extracted image was 100% and the NCC was 1.

3. PROPOSED METHOD

3.1.QR factorization

The QR factorization is widely used for finding all eigenvalues of a matrix. The matrix is first transformed into the Hessenberg matrix by an orthogonal similarity transformation, then the eigenvalue and eigenvector are obtained by the QR method. Gram-Schmidt orthogonalization is used in the decomposition process.

For any real matrix A, there are an orthogonal matrix Q and an upper triangular matrix R, such that [19]:

$$A = Q * R \qquad (1)$$

The above formula is called the orthogonal triangular decomposition of a matrix, also known as QR factorization.

3.2.Discrete Wavelet Transform

In Discrete Wavelet Transform (DWT), the wavelet coefficients matrix is applied to the data vector in a hierarchical algorithm. The wavelet coefficients are arranged in a form that odd rows contain an ordering of wavelet coefficients which act as the smoothing filter, and the even rows of the coefficient matrix contain an ordering of wavelet coefficient with different signs which act to bring out the data's detail. The resulted vector is decimated by half and the matrix may apply again and again. Each time the coefficient matrix is applied, a higher resolution is performed 20.

Applying DWT on an image of size $n \times n$ results in four sub-bands (LL, LH, HL and HH) each one is of size $\frac{n}{2} \times \frac{n}{2}$. L is for the low-pass filter and H is for the high-pass filter.

3.3. Main method

The main method depends on the QR factorization technique to hide an image

Published by Arab Journals Platform, 2021

within another image. The cover image is decomposed using QR decomposition. The same matrix decomposition is applied to the secret image and both matrices are embedded using a scaling factor. Inverse multiplication is applied to produce a stego-image. This is shown in Figure 1.

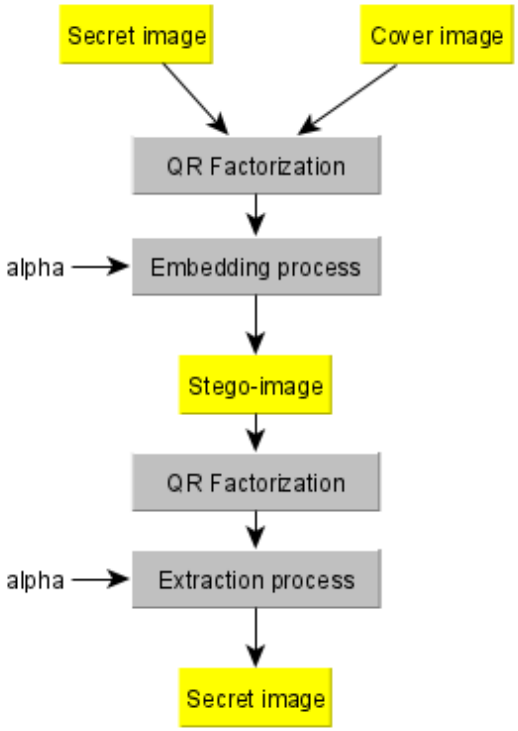


Figure. 1: Block diagram for the main algorithm.

3.4.Embedding process

Embedding process steps:

1- Read the cover image A_c
2- Apply matrix decomposition
$$[Q_c\ , R_c] = qr\ (A_c) \quad (2)$$
3- Read the secret image A_s
4- Apply same matrix decomposition
$$[Q_s\ , R_s] = qr\ (A_s) \quad (3)$$
5- Embed both matrices
$$R_n = R_c + (alpha \times R_s) \quad (4)$$
6- Produce the stego-image
$$si = Q_c R_n \quad (5)$$

3.5. Extraction process

Extraction process steps:

1- Read the stego-image si
2- Apply matrix decomposition
$$[Q_{si}\ , R_{si}] = qr\ (si) \quad (6)$$
3- Extract the embedded matrix
$$R_{new} = \frac{(R_{si} - R_c)}{alpha} \quad (7)$$
4- Output the secret image
$$secim = Q_s\ R_{new} \quad (8)$$

3.6. Enhanced method

The enhanced method depends on QR factorization and DWT to hide an image within another image. The cover image is transformed to wavelet domain using DWT and the resulted sub-band 'LL' is then decomposed using QR decomposition. The same matrix decomposition is applied to the secret image and both matrices are embedded using a scaling factor. Inverse multiplication is applied to produce a stego-image. In this method, the size of the secret image is half the size of the cover image. This is shown in Figure 2.

https://digitalcommons.aaru.edu.jo/fcij/vol6/iss2/2
DOI: http://doi.org/10.54623/fue.fcij.6.2.2

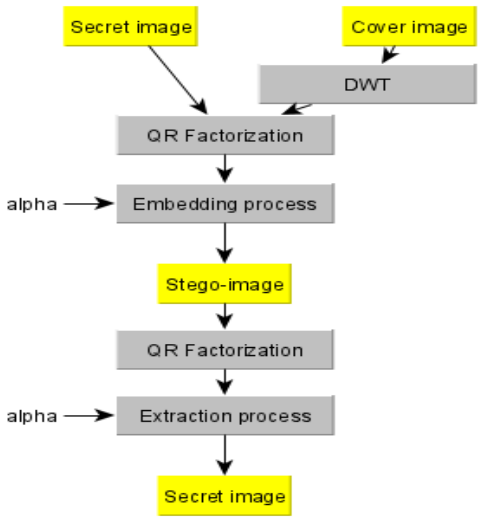


Figure 2: Block diagram for the enhanced algorithm.

4. RESULTS AND DISCUSSION

4.1. Performance criteria

1- Peak Signal to Noise Ratio

The visual performance of the stego-image and the secret image is measured using PSNR [21] and Structural Similarity Index Measure (SSIM) [21] presented in (10) and (11).PSNR calculates the ratio between two images. It depends on the Mean Square Error (MSE) in calculations. The MSE is computed as:

$$MSE=\frac{1}{xy}\sum_{i=0}^{x-1}\sum_{j=0}^{y-1}[M(i.j)-N(i,j)]^2 . \quad (9)$$

The PSNR is computed as:

$$PSNR = 10.\log_{10}\left(\frac{MAX_M^2}{MSE}\right). \quad (10)$$

where MAX is the maximum possible pixel value of the image, image M is a x × y matrix and N is its noisy approximation.

2- Structural Similarity Index

The Structural Similarity Index Measure (SSIM), measures the similarity between two images. It is calculated as:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} . \quad (11)$$

where x and y are two windows of common size,μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y and σ_{xy} is the covariance of x and y.

3- Normalized Cross-Correlation

The Normalized Cross-Correlation (NCC) calculates the cross-correlation depending on the size of the images. Then, it computes the local sums by pre-computing running sums. It uses local sums to normalize the cross-correlation to get correlation coefficients. The output matrix holds the correlation coefficients, which can range between −1.0 and 1.0. NCC is defined as [22]

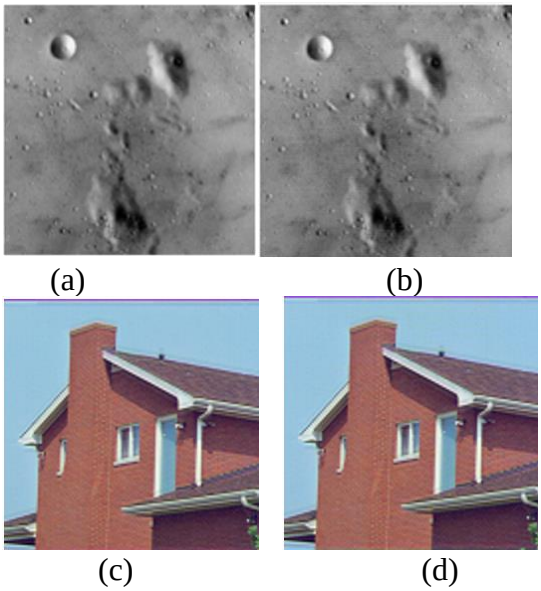
$$NCC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(P[i,j]\times S[i,j])}{\sum_{i=1}^{m}\sum_{j=1}^{n}(P[i,j])^2} \quad (12)$$

The NCC is more robust under uniform illumination changes. The value of NCC close to 1.0 represents the perfect quality of the stego-image.

4.2. Qualitative results

As shown in Figure 3, the human visual system cannot distinguish between the original cover images and the stego-images using the QR decomposition technique.

Published by Arab Journals Platform, 2021

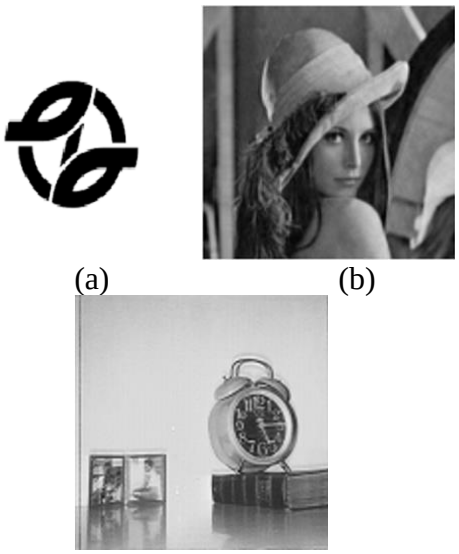


(a) (b)

(c) (d)

Figure 3: Comparison between the original cover image and the stego-image using QR factorization
(a)(c) the original cover images
(b) (d) the stego-images

Figure 4 display the extracted secret images using QR decomposition.



(a) (b)

(c)

Figure 4: The extracted secret images from QR factorization
(a) Logo (b) Lena (c) Clock

4.3. Quantitative results

Table 1 shows the performance of the proposed algorithm using QR factorization for different cover and secret images. The performance is measured using PSNR for the cover image and SSIM and NCC for the secret image.

Table 1: Performance of the algorithm using QR factorization

	Cover PSNR	Secret image SSIM	Secret image NCC
Moon + logo	41.4	1	1
Moon + lena	46.4	1	1
Moon + clock	42.7	1	1
House + logo	46.3	1	1
House + lena	51.44	1	1
House + clock	47.66	1	1

Table 2: Performance of the algorithm using QR factorization and DWT

	Cover PSNR	Secret image SSIM	Secret image NCC
Moon + logo	47.9	1	1
Moon + lena	51.9	1	1
Moon + clock	48.3	1	1
House + logo	52.9	1	1
House + lena	56.8	1	1
House + clock	53.2	1	1

As shown in Tables 1, the imperceptibility of the algorithm is very high as the cover PSNR is ranging from 41 to 51 dB. The cover PSNR is better when using the QR factorization with the DWT

https://digitalcommons.aaru.edu.jo/fcij/vol6/iss2/2
DOI: http://doi.org/10.54623/fue.fcij.6.2.2

rather than the QR factorization only. For the two methods, the secret image similarity and NCC is 1 which means that the secret image extracted without any distortion. The size of the secret image in the main method is 256×256 as the size of the cover image, but in the enhanced method, the size of the secret image is 128×128 the half size of the cover image. The enhanced method is more secure because of its complexity.

4.4. Comparative analysis

The algorithm is tested and the results are compared by the algorithm proposed by El-Shahed et al. [18]. Table 2 shows the comparison between the two algorithms in terms of cover PSNR.

Both techniques achieved 100% SSIM and NCC 1. But the proposed algorithm using QR factorization and DWT showed better results in terms of cover PSNR than the algorithm proposed by El-Shahed et al [18] which used LU Factorization.

Table 3: Performance of the algorithm compared to the algorithm proposed by El-Shahed *et al* [18]

	Proposed technique using QR factorization	Proposed technique using QR factorization and DWT	El-Shahed *et al.* [18] technique
Moon + logo	41.4	47.9	36.8
Moon + lena	46.4	51.9	40.3
Moon + clock	42.7	48.3	37.5
House + logo	46.3	52.9	42.5
House + lena	51.44	56.8	42.88
House + clock	47.66	53.2	44.09

5. Conclusion

Steganography is the art of hiding data. In steganography, the data is hidden in a cover object. The proposed technique is an image steganography technique, which hides an image in another image. The technique depends on the QR factorization technique to hides the secret image. The performance of the algorithm is measured using PSNR, SSIM and NCC. The PSNR of the cover image is ranging from 41 to 52 dB. The method is enhanced by combining DWT to the QR factorization and the PSNR of the cover image is ranging from 48 to 56 dB. The similarity between secret and extracted image is 100% and the NCC is 1 for both methods. But the size of the secret image is half the size of the cover image in the enhanced method. The comparative analysis showed that the performance of the algorithm is better than other state-of-the-art algorithms in terms of cover PSNR.

References

1. Farah Qasim Ahmed Alyousuf , Roshidi Din and Alaa Jabbar Qasim "Analysis review on spatial and transform domain technique in digital steganography" Bulletin of Electrical Engineering and Informatics Vol. 9, No. 2, April 2020, pp. 573~581
2. Mehdi HussainAinuddin Wahid Abdul WahabYamani Idna Bin IdrisAnthony T.S and HoKi-Hyun JungFig. "Image steganography in spatial domain: A survey" Signal Processing: Image Communication, Volume 65, 2018, Pages 46-66,
3. Chan C.-K. and Cheng L.-M "Hiding data in images by simple LSB substitution" Pattern Recognit., 37 (2004), pp. 469-474

4. Wu D.-C. and Tsai W.-H. "A steganographic method for images by pixel-value differencing" Pattern Recognit. Lett., 24 (2003), pp. 1613-1626
5. Zhang X. and Wang S. "Efficient steganographic embedding by exploiting modification direction" IEEE Commun. Lett., 10 (2006), pp. 781-783
6. Afrakhteh M. and Ibrahim S. "Adaptive steganography scheme using more surrounding pixels" Computer Design and Applications, ICCDA, 2010 International Conference on, IEEE (2010) pp. V1-225-V221-229
7. Hong W. and Chen T.-S. "A novel data embedding method using adaptive pixel pair matching" IEEE Trans. Inf. Forensics Secur., 7 (2012), pp. 176-184
8. Potdar V.M. and Chang E. "Grey level modification steganography for secret communication" Industrial Informatics, 2004 INDIN'04 2004 2nd IEEE International Conference on, IEEE (2004), pp. 223-228
9. Yu Y.-H., Chang C.-C. and Hu Y.-C. "Hiding secret data in images via predictive coding" Pattern Recognit., 38 (2005), pp. 691-705
10. Tsai P., Hu Y.-C. and Yeh H.-L. "Reversible image hiding scheme using predictive coding and histogram shifting" Signal Process., 89 (2009), pp. 1129-1143
11. Luo W., Huang F. and Huang J "Edge adaptive image steganography based on LSB matching revisited" IEEE Trans. Inf. Forensics Secur., 5 (2010), pp. 201-214
12. Wang R.-Z. and Chen Y.-S "High-payload image steganography using two-way block matching" IEEE Signal Process. Lett., 13 (2006), pp. 161-164
13. Muhammad K., Sajjad M., Mehmood I., Rho S. and Baik S.W. "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks" Future Gener. Comput. Syst. (2016)
14. Kamaldeep Joshi, Swati Gill, Rajkumar Yadav. A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image, Journal of Computer Networks and Communications, vol. 2018, 2018.
15. NamitaTiwari, Madhu Sandilya and Meenu Chawla "Spatial Domain Image Steganography based on Security and Randomization" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014
16. Firas A. Jassim "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method" International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, June 2013
17. Ali Ahmed and Abdelmotalib Ahmed "A Secure Image Steganography using LSB and Double XOR Operations" IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.5, May 2020
18. El-Shahed, Reham A., Al-Berry, M. N., Ebeid, Hala M. and Shedeed, Howida A., Image hiding using upper-lower decomposition technique. International Journal of Intelligent Computing and Information Sciences (IJICIS) (Accepted)
19. Qingtang Su, Yugang Niu, Gang Wang, Shaoli Jia and Jun Yue, Color image blind watermarking scheme based on QR decomposition. Signal Process. Vol. 94, 2014, pp. 219–235
20. G., Amara. "An Introduction to Wavelets." IEEE computational sciences and engineering, vol. 2, pp. 50-61, 1995.

https://digitalcommons.aaru.edu.jo/fcij/vol6/iss2/2
DOI: http://doi.org/10.54623/fue.fcij.6.2.2

21. A. G. George, A. K. Prabavathy : A survey on different approaches used in image quality Assessment international journal of emerging technology and advanced engineering. 3(2), 2013 197-203

22. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Trans. Image Process, 13, 2004, 600–612