Authentication of Digital Media Using Reversible Watermarking

Geeta Sharma, Vinay Kumar, and Kavita Chaudhary

Abstract Digital watermarking is a technique to hide and transmit the data in such a manner that attackers cannot perceive it. The watermarks can be used for authentication, and the creator/owner of the digital data can claim the rights, in case of any dispute. The reversible digital watermarking ensures the reusability of the cover media. In this research paper, we are suggesting a more robust method of watermarking using the combination of LWT-SVD. The digest of the message is generated using MD5 algorithm, and a quantum representation is used as the trap door. The results are measured for the existing quantum technique, LSB quantum watermarking, and the proposed algorithm. We have compared the results for MSE, SSIM, and PSNR in the analysis section. The improvements can be seen in the results persistently.

Keywords Digital watermarking · DWT · Singular value decomposition · Quantum representation

1 Introduction

Multimedia, Internet of things and the Web of digital devices around us are rapidly generating digital data. This data need to be protected in such a manner that no unintentional receivers can even perceive the very presence of the data. Digital watermarking provides a strong method for information hiding as data is stored in the cover in non-perceivable manner and the process can be reversed by the intended users with security information provided by the sender. A digital water-

G. Sharma (✉)
IP University, Delhi, India
e-mail: geeta.sharma@jimsindia.org

V. Kumar
NIC, Delhi, India

K. Chaudhary
Jagannath University, Jaipur, India

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_6

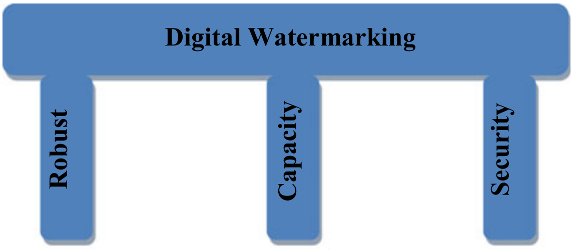


Fig. 1 Three pillars

marking technique has three major parameters that are robustness, capacity, and security as in Fig. 1. Robustness indicates that any kind of attacks will not affect the watermark much. Capacity is the maximum information that the cover can hold. Security, as name suggests, refrains the unauthorized access. Another important parameter is reversibility of the watermarking process that allows the use of cover image at the receiver's end.

The lifting system is an efficient way of implementing wavelet filtering, which also increases the wavelet transformation process speed. The prediction stage of the lifting scheme for the Haar transform predicts that the each odd element will be equal to its even element. The dissimilarity between the even value (the predicted element) and the original value of the odd value restores an odd element. The basics of the work is already discussed in [1].

2 Literature Review

Digital watermarking technique/algorithms can be characterized on the basis of many factors. The cover that is used for the information hiding can be text, image, sound, video, etc. A watermark can be visible or invisible, according to capacity of human eye to perceive. An invisible watermark can be fragile and robust both. Since fragile means imperceptible, it can be further divided into fragile and semi-fragile categories. The process of data hiding can be reversible and irreversible. In reversible data hiding, the cover can be used by the receiver after extracting the watermark. Watermarking is divided into two main groups: spatial domain and transform domain. Now, we will discuss few papers that helped in understanding and formed a base of the research.

For image steganography, the suggested technique is a mixed method that combines discrete wavelet transform (DWT) along with singular value decomposition (SVD) and lifting wavelet transform (LWT) techniques.

2.1 Discrete Wavelet Transform

In digital images, the discrete wavelet transform is used. There are several DWTs accessible. The most acceptable one should be used, depending on the application. Integer wavelet transformation can be used to cover text details. When DWT is applied to an image, it divides it into four sub-bands: LL, HL, LH, and HH. The first section (LL) consists of the most critical features. So if the data is hidden in the LL section, the compression or other changes do not affect the stego image to great extent. In the stego picture, distortion can sometimes be created and now other sub-bands can be used. The expanded function is discrete (i.e., a number sequence), and the resultant coefficients are named discrete wavelet transformation (DWT).

"Thakkar and Srivastava" [2]: "A blind image watermarking technique based on DWT and SVD was developed in this paper. The DWT technique was used in the medical image's Region of Interest. On the low-frequency sub-band LL-ROI, the program Block-SVD was used to obtain separate singular matrices. A pair of elements with identical values was discovered using either the left singular value matrix of all of the selected blocks. Using some criterion to embed a bit with watermark information, their properties of these pairs are changed. In order to achieve that imperceptibility of the medical image with watermark material, acceptable thresholds were selected."

"Zear et al." [3]: "Throughout this study, an algorithm with multiple watermarking based on discrete wavelet transformations (DWT), discrete cosine transformation (DCT), and singular value decomposition (SVD) was proposed for healthcare applications. The suggested application uses a total of three watermarks: a medical 'Lump picture watermark,' a code for the doctor's signature, and the patient's diagnosis details as text watermarks for identity authentication. Back Propagation Neural Network (BPNN) was used on both the derived watermark i.e. image format and the image watermark to reduce the potential impact on the watermarked image and to increase the image watermark's robustness."

2.2 Quantization-Based Watermarking

In 1984, Bennett and Brassard presented the first quantum key distribution protocol. Since then it was used in many theories-based and/or practical research. In the traditional method, a computer stores the pixel representation of the image with the necessary color information and the corresponding coordinates of each point. The same method was used by Shahrokh and Mosayeb [4], and the picture information is converted into the quantum state. The basic unit of quantum information is known as quantum bits (qubits).

Nezhadarya et al. [5]: "This paper proposed a robust picture watermarking framework based on quantization, referred to as quantization-based authentication path watermarking (GDWM), with a focus on uniform gradient vector direction quantization. The watermark bits become embedded in GDWM through quantifying vector angles and critical gradient vectors on many wavelet scales. The current technique had the following key features: (1) increased invisibility of both embedded watermarks, owing to the fact that watermarks were embedded in major gradient vectors, (2) strength against amplitude scaling attacks, owing to the fact that watermarks were embedded across the entire gradient vector angles, and (3) increased watermarking capability, owing to the method's ability to allow multiple-scale embedding. Throughout recognition of both the discrete wavelet transform (DWT) coefficients, that gradient vector at one pixel was expressed. The DWT coefficients were updated to quantize that gradient direction mostly on resultant relationship here amongst changes during the coefficients or the modification in the gradient direction."

Sachdeva and Kumar [6]: "Digital images are most prevalent cover files used only for steganography would those be. In this article, a current format of steganography called JMQT were introduced based on an updated table of quantization. It method of steganography has been contrasted with the JPEG-JSteg method of steganography. Two output parameters are being contrasted, namely capability and stego scale. Existing customers and stego scale represents the amount. Therefore, JMQT offers better power and JPEG-JSteg offers better stego-size."

2.3 Singular Value Decomposition

Through the discernment of image processing, a picture can be interpreted as a matrix of non-negative scalar entries. The SVD method for decomposing a rectangular matrix "A" into an orthogonal matrix U, a diagonal matrix S, and transposing an orthogonal matrix V is an efficient linear algebra numerical analysis method. Through image processing, SVD decomposes a given image A of size MN as decomposition (SVD) of A, which is interpreted as a matrix of non-negative scalar entries. The SVD method for decomposing a rectangular matrix "A" into an orthogonal matrix U, a diagonal matrix S, and transposing an orthogonal matrix V is an efficient linear algebra numerical analysis method. A given image A of size MN is decomposed as decomposition (SVD) of A using SVD.

"Ali et al." [7]: "By analyzing multiple scaling variables in image watermarking, a Differential Evolution (DE) algorithm has been used to balance the trade-off between robustness and imperceptibility in this article. To begin, the original image was divided into blocks, which were then transformed into discrete cosine transformation domains (DCT). The DC coefficients from each block were used to create a low-resolution approximation image, which was then subjected to the Singular Value Decomposition (SVD) algorithm. After that, the watermark was merged by replacing the singular values of both watermarks with the singular values of both watermarks."

“Du et al.” [8]: “In order to ensure the copyright of a color image, a robust image watermarking approach based on ‘Tensor-Singular Value Decomposition (T-SVD)’ was proposed. The color image was created by transforming the third-order tensor with T-SVD to produce three orthogonal tensors and a diagonal tensor in order to establish clear associations between the three RGB color image channels. Because the main energies of that color picture are contained in the diagonal tensor, robustness can be used and the watermark can be embedded. Second, three color image channels were decomposed into four sub bands using discrete wavelet transformation (DWT), but only the LL sub band of each channel was used to create an approximate image. In addition, the approximation picture was divided into non-blocks of 4 × 4 dimensions, and the first, second, and third diagonal matrices were calculated using TSVD from each block. Finally, singular value decomposition was used to decompose the grayscale watermark (SVD).”

3 Method Proposed

Based on the standard existing algorithm, this proposed algorithm is similar to performing. The embedding is performed on the images, generally a loss less file format is used. The DWT method is combined with the benefits of SVD for embedding the image. The quantum representation is used as the trap door to fetch the watermark without changing the picture information of the cover. So the embedding ability and image quality are enhanced effectively by this algorithm. The ability for embedding is doubled over and the graphical output is greatly enhanced. The recommended reversible image watermarking algorithm largely helps increase the embedding rate of the watermark while retaining better visual quality than other algorithms.

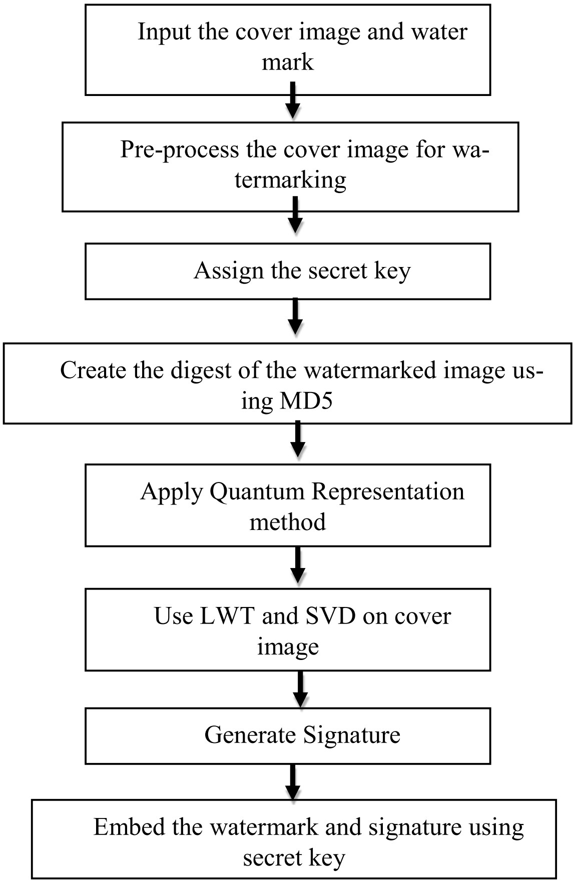
3.1 Embedding Algorithm

This function extracted the watermark without damaging the cover image, using the cover image, watermark/hidden message, key, signature as an input. The flow of the function is explained in Fig. 2.

Step 1: Import cover image and watermark (image).
Step 2: For each channel apply following to the cover image:

(a) Resize image to 512 × 512 using bilinear algorithm.
(b) Assign a random key (secret key).
(c) Get the non-negative integer seed key.
(d) Assign 10 to QR block size.

Fig. 2 Flowchart of the embedding algorithm


Input the cover image and water mark
Pre-process the cover image for watermarking
Assign the secret key
Create the digest of the watermarked image using MD5
Apply Quantum Representation method
Use LWT and SVD on cover image
Generate Signature
Embed the watermark and signature using secret key

Step 3: Apply quantum representation on secret image using MD5.
Step 4: Convert watermark to B&W and apply following operations on watermark:

(a) Decompose the watermarked image or signal into four sub-bands, using Haar wavelet.
(b) Apply DWT on LL band up to fourth level.
(c) Also perform single value decomposition (SVD) to the high-frequency band (HH) of the watermark.

Step 5: Also decompose the watermarked image using SVD and replace values of HH band with SV of the watermark.
Step 6: Generate signature using values from watermark and key, and then embed the signature in LL band of the cover.
Step 7: After getting the updated HH band of cover image, finally acquire the watermarked image by applying inverse LWT.

3.2 Extraction Algorithm

Step 1: Import watermarked image (cover image + watermark embedded as single unit).
Step 2: Apply following operations on the watermarked image:

(a) Convert the watermarked image into four sub-bands, using Haar wavelet.
(b) Apply LWT on LL band up to fourth level.
(c) Also perform single value decomposition (SVD) to the high-frequency (HH) band.

Step 3: Generate signature using matrices of the watermarked image.
Step 4: Reconstruct the signature from the fourth level LL an HH band.
Step 5: Compare these signatures and follow these steps if the user is authenticated, else the extraction process should be stopped:

(a) Apply SVD to the HH band.
(b) Get the singular values from the HH band.
(c) Now, get the watermark image using orthogonal matrices and singular values.

Step 6: The watermark and the cover image both are in useable forms.

4 Analysis

Authentication and copyright management are two of the most common uses for reversible digital watermarking. In the field of image steganography, many studies have been conducted using the discrete wavelet, lifting scheme, and singular value decomposition. During our research, we examined the outcomes of various variations before settling on the most promising technique. We have taken into account the results of quantum steganography, LSB quantum watermarking, and LWT-QR-MD5 for this analysis.

The image Fig. 4 is clearly showing the high correlation between the input image and the resultant image. This high correlation indicates that embedding of the watermark to the cover image is not making much difference in the actual image that further ensures the better imperceptibility. As we discussed earlier, if a watermark is not able to perceive easily than it automatically reduce the number of attacks. It is also visible in the histogram of the image in Fig. 3. Now, we will use the algorithm on the basic three images Lena, Barbara, and Peppers and see the results.

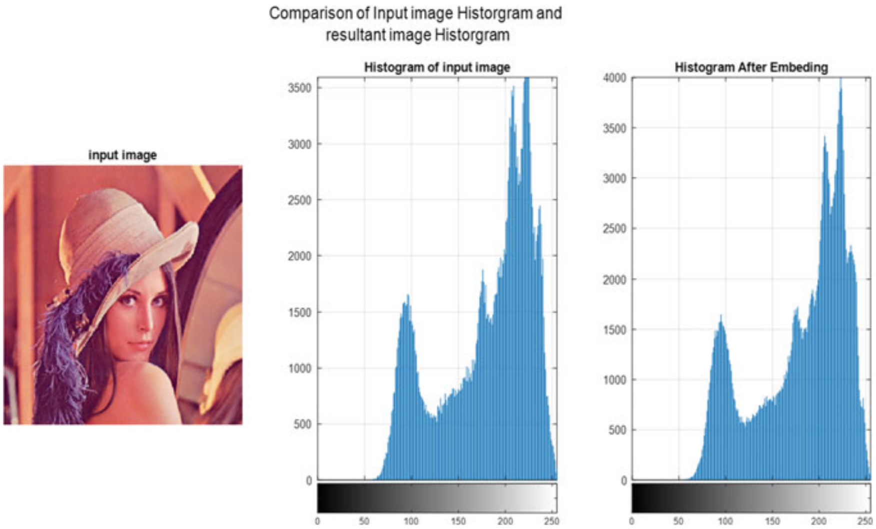


Fig. 3 Comparison of original and resultant image “Lena”

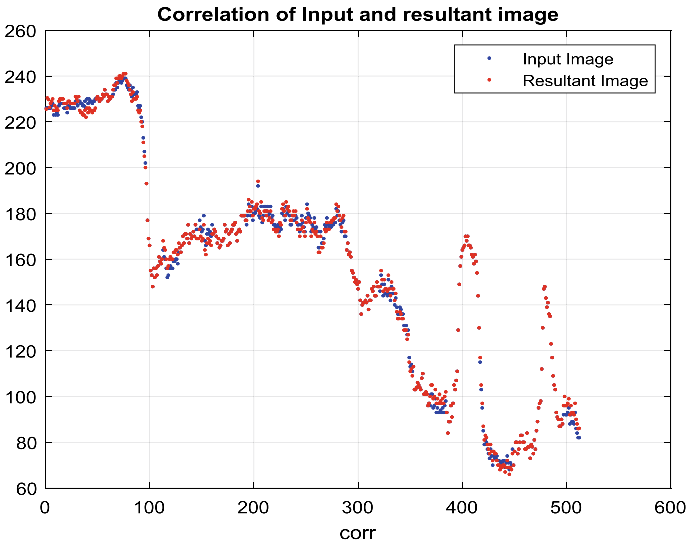


Fig. 4 Depiction of correlation

4.1 PSNR

It is used to check and compute the strength of the signal [9]. Figure 5 is showing the PSNR results after improvement in absolute term and percentage have been

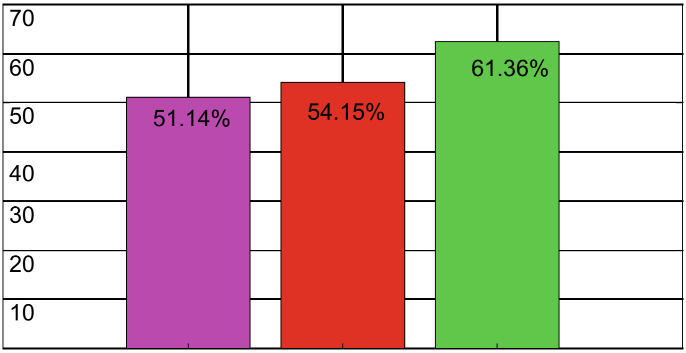


Fig. 5 Mean value of PSNR

Table 1 PSNR results

Image	Quantum steganography	LSB quantum watermarking	LWT-QR-MD5	PSNR improvement	% Improvement
Lena	51.1789	54.24	62.69	8.44	15.6
Barbara	51.0889	54.10	59.94	5.85	10.8
Peppers	51.1549	54.13	61.44	7.31	13.5
Average	51.1409	54.156	61.356	7.2	13.3

found that mean value of the PSNR applied on the various images like Lena, Barbara, and Peppers. The comparison was made for the three algorithms, i.e., quantum steganography, LSB watermarking, and the proposed algorithm. If we look at the average improvement of the resultant images, there is a clear increase of more than 13% that is a significant improvement (Table 1).

4.2 MSE

It is used to see how closely the original image and the watermarked image resemble each other [10]. This discrepancy is then squared, according to Wikipedia. Yi denotes the pixel position in the original image and Yi denotes the pixel value in the watermarked image at the same location. The MSE value is then computed by multiplying the difference by two [11]. Table 2 presented the mean square error results after applied proposed algorithm with LSB quantum watermarking, LWT-QR-MD5, MSE improvement, % improvement with three images. It was found that image Lena was showed that LSB quantum watermarking was 24.69, LWT-QR-MD5 8.14, MSE improvement 16.55, and it increased up to 67.02%, respectively (Fig. 6).

Table 2 MSE results

Image	LSB quantum watermarking	LWT-QR-MD5	MSE improvement	% Improvement
Lena	24.69	8.14	16.55	67.02
Barbara	25.50	11.75	13.74	53.91
Peppers	25.32	17.09	8.24	32.52
Average	25.17	12.32	12.84	51.15

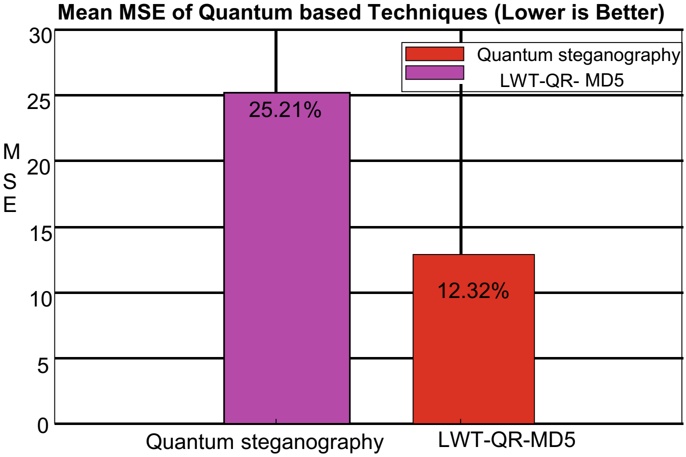


Fig. 6 Mean of MSE

It was found that image Barbara was showed that LSB quantum watermarking was 25.50, LWT-QR-MD5 11.75, MSE improvement 13.74, and it increased up to 53.91%, respectively. It was found that image Peppers was showed that LSB quantum watermarking was 25.32, LWT-QR-MD5 17.09, MSE improvement 8.24, and it increased up to 32.52%.

4.3 SSIM

Structural similarity (SSIM) was used to calculate the similarity between the filtered residual images and original images [12]. From Table 3 presented, we can observe the improvements in SSIM improvements. The three images were observed under LSB quantum watermarking, LWT-QR-MD5, SSIM improvement, and % improvement. It was found that Lena was showed that LSB quantum watermarking was 81.53, LWT-QR-MD5 93.71, SSIM improvement 12.18, and it increased up to 14.94%, respectively. It was found that Barbara was showed that LSB quantum watermarking was 84.33, LWT-QR-MD5 95.83, SSIM improvement 11.50, and it

Table 3 SSIM results

Image	LSB quantum watermarking	LWT-QR-MD5	SSIM improvement	% Improvement
Lena	81.53	93.71	12.18	14.94
Barbara	84.33	95.83	11.50	13.64
Peppers	82.69	89.88	7.19	8.70
Average	82.85	93.14	10.29	12.29

increased up to 13.64%, respectively. It was found that Peppers was showed that LSB quantum watermarking was 82.69, LWT-QR-MD5 89.88, SSIM improvement 7.19, and it increased up to 8.70%, respectively.

5 Conclusion and Future Scope

Watermarking is typically used to include evidence of digital data control. Generally, that is done by integrating certain copyright knowledge into digital details. Since it can be found on the World Wide Web for automated tracking of copywrite products. The algorithm suggested is capable of retrieving the secret message without making significant changes to the cover image. For authentication and copyright management, reversible automated watermarking is largely utilized. Through the usage of quantum watermarking, LWT-QR-MD5 techniques, this loss less approach ensures the improvement in the existing algorithms.

LWT promises faster computation while consuming less memory. Furthermore, the MD5 algorithm ensures better security and improves the algorithm's robustness against various attacks. In the steg analysis, this reversible watermarking technique produces better results. In future, we are planning to apply the same algorithm on more images and will also execute some attacks on the watermarked image.

References

1. Sharma, G., Kumar, V.: Review of different parameters for digital reversible watermarking. Int. J. Res. Anal. Rev. (2018). E-ISSN 2348–1269, P- ISSN 2349–5138
2. Thakkar, F.N., Srivastava, V.K.: A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools Appl. **76**(3), 3669–3697 (2017)
3. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools Appl. **77**(4), 4863–4882 (2018)
4. Shahrokh, H., Mosayeb, N.: A Novel LSB based quantum watermarking. Int. J. Theor. Phys. Springer Science + Business Media New York (2016)

5. Nezhadarya, E., Wang, Z.J., Ward, R.K.: Robust image watermarking based on multiscale gradient direction quantization. IEEE Trans. Inf. Forensics Secur. **6**(4), 1200–1213 (2011)
6. Sachdeva, S., Kumar, A.: Colour image steganography based on modified quantization table. In: 2012 Second International Conference on Advanced Computing and Communication Technologies, pp. 309–313. IEEE (2012)
7. Ali, M., Ahn, C.W., Pant, M.: A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik **125**(1), 428–434 (2014)
8. Du, M., Luo, T., Li, L., Xu, H., Song, Y.: T-SVD-based robust color image watermarking. IEEE Access **7**, 168655–168668 (2019)
9. Jadhav, A., Kolhekar, M.: Digital watermarking in video for copyright protection. In: 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), pp. 140–144. IEEE (2014)
10. Lou, D.C., Chou, C.L., Tso, H.K., Chiu, C.C.: Active steg analysis for histogram-shifting based reversible data hiding. Optics Commun. **285**(10–11), 2510–2518 (2012)
11. Botta, M., Cavagnino, D., Pomponiu, V.: A modular framework for color image watermarking. Sig. Process. **119**, 102–114 (2016)
12. Song, C., Sudirman, S., Merabti, M., Llewellyn-Jones, D.: Analysis of digital image watermark attacks. In: IEEE CCNC 2010 Proceedings (2010)
13. Le, P.Q., Iliyasu, A.M., Dong, F., Hirota, K.: A flexible representation and invertible transformations for images on quantum computers. In: Ruano, A.E., Várkonyi-Kóczy, A.R. (eds) New advances in intelligent signal processing. Studies in Computational Intelligence, vol. 372. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-11739-8_9