Robust Watermarking Method using QIM with VSS for Image Copyright Protection

Thanh Ta Minh, Dan Giang Ngoc
Le Quy Don Technical University
Correspondence: Ta Minh Thanh, thanhtm@lqdtu.edu.vn
Communication: received 30 October 2020, revised 4 April 2021, accepted 31 May
Digital Object Identifier: 10.32913/mic-ict-research.v2021.n1.971

***Abstract*: This paper proposes a new watermarking method for digital image by composing the DWT-QIM based embedding with visual secret sharing (VSS) method. Firstly, the watermark image is separated into n shares by using the k-out-of-n method, also called (k,n) visual secret sharing. One of the s is embeded into the original image for copyright protection. The other (n-1) shares are registered with Vietnam Copyright Department. When a dispute happens, the verifier can extract the watermark information from the watermarked image, then, decode it with (k-1) shares chosen from (n-1) shares to retrieve the copyright information. Our experimental results show that our proposed method works efficiently on protecting the copyright of digital images.**

Keywords: *Image watermarking, copyright protection, digital content, visual secret sharing - VSS, (k,n) sharing method.*

I. Introduction

1. Overview

The industrial revolution 4.0 has changed people's perception, as well as the way people approach and communicate with each other on the Internet. The advent of software and new devices such as digital cameras, high-quality scanners, printers, digital audio recorders, etc. has allowed the vast consumer world to create, process and enjoy multimedia data. Along with the development of social networks, the Internet has become a "virtual society" where information exchange takes place in all fields such as politics, military, national defense, economy, and commercial. It is in such an open and comfortable environment that issues such as piracy, information misrepresentation, and unauthorized access to digital multimedia arise. Therefore, a solution to protect digital products, preserve information, and protect copyright for digital products is urgently required. Among the current solutions, digital watermarking is one that is being researched because of its effectiveness and suitability for copyright protection of multimedia products.

In our recent proposal [23], we mentioned a watermarking method based on a combination of Discrete Wavelet Transform (DWT) and cryptographic techniques Visual Secret Sharing (VSS). The experimental results with that proposal have demonstrated that the above combination has enhanced the imperceptibility after embedding the watermark, as well as the stability of the watermark against some common digital transformations. However, that solution still has some limitations such as needing the original image in the process of extracting copyright information, which is known as non-blind watermarking.

Inheriting the results from previous studies, we continue to propose an improved watermarking method, with the combination of DWT-QIM and VSS. The difference in this algorithm is that the embedding and extraction of watermarks will be conducted in a smarter way, closer to the actual application through the use of quantization index modulation (QIM) to adjust image quality and persistence of copyright information.

Normally, for a digital watermarking method to be effective, it needs to be hidden and robust against common image manipulations such as compression, filtering, rotation, scaling, collusion attacks, and so on. Many other digital signal processing operations also need to be guaranteed. Current digital image watermarking techniques can be classified into two groups: spatial domain watermarking techniques and frequency domain watermarking techniques [14]. Compared to the spatial domain watermarking technique, the frequency domain watermarking technique proves more effective in achieving the hiddenness and robustness requirements of the digital watermarking algorithm.

Commonly used frequency domain transforms include Discrete Wavelet Transform (DWT), Discrete Consine Transform (DCT) and Discrete Fourier Transform (DFT). The proposed sustainable watermarking techniques on the frequency domain of the image have attracted attention in recent years because of their feasibility and effectiveness in copyright protection applications such as watermarking techniques on frequency domain DCT[1-3], frequency domain DWT [4-7], and frequency domain DFT [8-9]. Frequency domain watermarking solutions have shown advantages in creating sustainable watermarking solutions, suitable for digital product copyright protection applications. Frequency domain watermarking techniques are often chosen to suit products affected by techniques such as compression, which will be applied to the DCT frequency domain watermarking solution foto improve the image quality. However, DWT is used in digital image watermarking more often because of its spatial localization and multi-resolution characteristics. Its solution is similar to the theoretical model of the human visual system (HVS). Better performance improvements in DWT-based digital image watermark algorithms can be achieved in many ways to suit different digital product objects such as digital music, digital movies, and digital images.

To balance the improvement of digital image quality after watermark embedding and the stability of watermark information, research on extended frequency domains such as q-DCT [10], q-DWT [11], or q-SVD [12] is also proposed to balance these two goals. However, adjusting the parameter value q to satisfy the condition of balancing both criteria is difficult to achieve. The authors had to evaluate the image quality after embedding and the durability of the watermark to choose the most appropriate value for the parameter q. Although the computational complexity of these proposals still needs improvement, it opens up a new frequency domain research direction applied in digital watermarking proposals.

Another technique to protect digital image copyright is zero watermarking technique, in which the watermark information will not be directly embedded in the digital image, but the stable features of the digital image will be extracted for encoding with copyright information to generate information registered with the Copyright Office[13]. However, zero watermarking depends heavily on the properties and characteristics of the digital image. For images with large “complexity”, the extracted feature will be resistant to image attacks.

In this paper, we focus our research on embedding and extracting watermark algorithms based on quantization index modulation (QIM) combined with visual secret sharing (VSS) to improve the inequalities. Our proposed method can recognize and enhance the stability of the watermark after it is extracted, and at the same time ensure that the watermark can be sufficiently resistant to normal image transformations.

2. Our contribution

We summarize the problem to be solved in the proposal of the new digital watermarking technique as follows:

Most watermarking application solutions are used to protect digital product and copyright verification. However, copyright information, after being embedded in digital products, requires resistance to image attacks to verify ownership when a dispute occurs. Our paper proposes an idea to combine visual secret sharing (VSS) with watermarking techniques to improve the stability of watermarks after being hidden in digital images. The use of an intuitive encryption system combined with scrambled encryption has helped our proposal improve the security of copyright information, creating reliability for users when participating in the solution.

3. Roadmap

In this paper, we organize the content as follows: The knowledge related to our proposed method is presented in Section II. The architecture and detailed description of the proposed model are presented in Section III. The experimental and evaluation results are presented in Section IV. Section V presents conclusions and future research proposals.

II. Related works

The watermarking method is based on the discrete wavelet transformation (DWT), which has been widely used in digital signal processing applications. The method in [23] effectively utilizes the property of discrete wavelet transform to improve the robustness of watermark information. However, when extracting watermarks from hidden images, it is necessary to have the same initial data as the original image. In fact, we are not always qualified to collect such data. Therefore, in this paper, we propose a better solution for the DWT transformation, which is to use quantization index modulation (QIM).

Visual Secret Sharing (VSS), is an encryption technique in which visual information (images, text, etc.) is encrypted so that decryption can be performed based on the human visual system. In this section, we briefly introduce these two techniques and outline their relevance to the implementation of watermarking on digital images.

1. Visual secret sharing - VSS

The overview of visual secret sharing (VSS) can be shown in Figure 1. VSS may share confidential information to protect the confidentiality of copyright information [15].

The idea of secret sharing was proposed by Adi Shamir [16] and G.Blakley [18] in 1979. Four years later, another method of secret sharing was proposed by Asmuth. and Bloom [19] in 1983. Accordingly, Shamir’s scheme is based

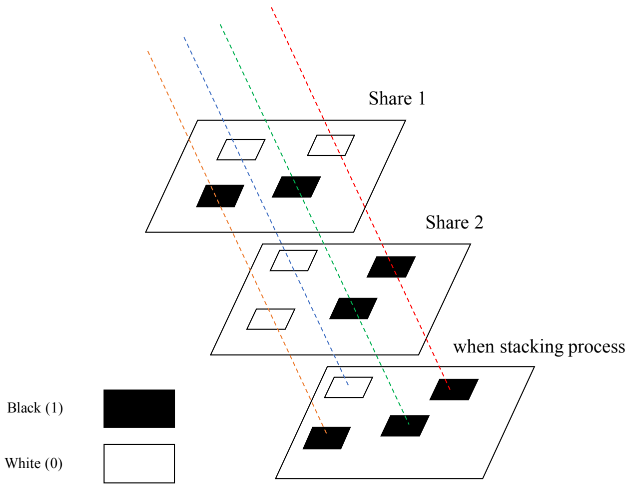


Figure 1. The human visual system functions as an OR-operator

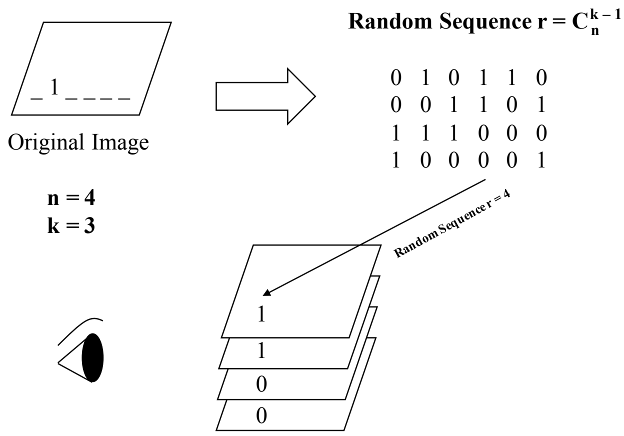


Figure 3. String value at position $pix(w, h)$

Figure 4. Sample shares created with $k = 6$ and $n = 10$

on polynomial interpolation, Blakley's scheme is based on hyperplane geometry, and Asmuth and Bloom's scheme is based on the Chinese remainder theorem.

In particular, the secret sharing scheme of Adi Shamir is considered the most potential in the field of image copyright protection. The basis of this proposal is to divide the image into secret shares (also known as Shares or Shadows). Each of these shares is treated as a random image generated from the original image. To reconstruct the original image, we simply combine these shares together as shown in Figure 2.

In this paper, we use the (k, n) secret sharing scheme based on random sequence (Random Sequence) [20]. In the schema (k, n), suppose we have a set P consisting of n elements, a secret image S (Secret Image) encrypted in these n elements. For each element in set P, we get a secret share. For any k secret share fragment (with $2 < k < n$) stacked, the secret image S will be reconstructed.

Figure 2. Adi Shamir's Secret Sharing Scheme

The secret sharing scheme (k, n) is based on a random sequence, which is a secret image scattering technique using randomly arranged strings of [0,1] values. Where, a random string is composed of $(n - k + 1)$ value "1" and $(k - 1)$ the value "0". For a secret image distributed with the scheme (k, n), the number of random strings (ns) is calculated by the convolution $(k - 1)$ of the n part death.

When viewed from the side with the secret shares stacked, the string value at $pix(w, h)$ (with $pix(w, h)$ on the original image having the value "1") is made up of $(n-k+1)$ value "1" and $(k - 1)$ value "0" as visually described in Figure 3. The result after scattering the watermark with $k = 6$ and $n = 10$ is shown in Figure 4.

2. Discrete wavelet transform - DWT

The discrete wavelet transform (DWT) on the digital image [17, 21-23] is shown in Figure 5. When first two-dimensional DWT transform on image I, the image I will be analyzed into frequency domains LL (Low-Low), LH (Low-High), HL (High-Low) and HH (High-High). These frequency domains will be used to embed watermark information based on the purpose of data hiding, invisible watermarking, or visible watermarking. Normally, the DWT frequency transform domain is used to embed copyright information, after the reverse transformation of IDWT (Inverse DWT), the copyright information will be distributed over the entire image surface, creating a persistence for copyright information hidden in images. Thus, from 4

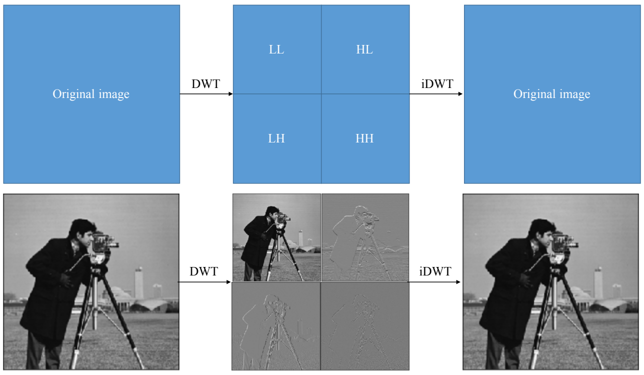


Figure 5. Discrete wavelet transform on digital image

subimages (LL, HL, LH, HH) shown in Figure 5, through the IDWT inverse transformation, we receive image I.

In this paper, we apply the DWT frequency transformation to obtain the frequency domain of pixels. After that, we proceed to embed the distributed watermark information on the DWT frequency region to ensure the stability of the embedding method.

3. DWT based watermarking methods

Recently, studies on frequency domain watermarking techniques are being widely proposed with the aim of overcoming the limitations of traditional frequency domain watermarking methods. Research in this field has thought of a solution that is to combine multiple watermarking methods.

In a study by Nawaf Hazim Barnouti, Zaid Saeb Sabri and Khandoun L. Hameed [25], the authors proposed a watermarking method based on the combination of two transformations - Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). In the paper, the authors have shown that the combination of two transformations, DWT and DCT, has brought a watermarking method that has the advantages of both transformations and has improved the performance compared to the simple methods. However, the implementation process of the authors has converted the original image from color image to gray image. This reduces the practicality of the proposal. Also, it has not been proven that this method can improve the robustness of the watermark against conventional image attacks.

Our most recent proposal [23] also proposed a watermarking method that combines DWT transformation and visual cryptography (VSS). That study also evaluated the effect of the above combination through two properties "Unrecognizability" and "Sustainability". The output helps to ensure the stability of the watermark against common

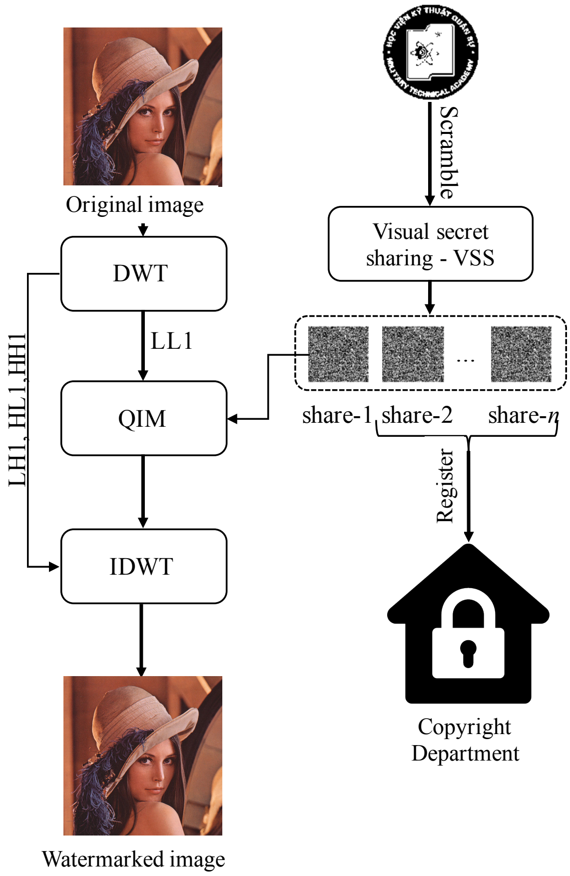


Figure 6. Watermark embedding algorithm combined with VSS

attacks, and at the same time, it is undetectable to the human eye after the watermark is embedded into the digital image. However, we realize that the above watermarking method is still not perfect, specifically, we still need to use the original data when extracting the watermark. This also reduces the level of applicability of the method.

III. Proposed QIM watermarking algorithm combined with VSS

In this section, we present a combination that is considered to be smarter and more practical with the combination of DWT-QIM and VSS. QIM combined with watermark scheme on DWT frequency domain is not a new idea, but in our paper, watermarking combined with QIM on DWT frequency domain will be applied to embedding distributed watermark using VSS to form a schema with the properties of zero watermark to overcome the limitations mentioned in section I.2.2. With this combination, we have overcome the limitations of the proposed method of watermarking combined with traditional DWT and VSS.

1. Watermark embedding algorithm combined with VSS

The input data of the embedding process includes: 01 cover image and 01 binary image to make the copyright watermark. The watermarked image is processed with scramble and visual cryptographic techniques to disperse the scrambled watermark image into different shares. Therefore, each share will not display any information. One share will be selected to embed in the cover image, and the remaining shares will be sent to a 3rd party in charge of copyright protection. After the watermark embedding process, we obtain the watermarked image. The watermark embedding process is visually described in Figure 6. The watermark embedding process is carried out according to the following steps:

Step 1: Input: Cover image, copyright logo.

Step 2: Scramble the copyright logo image by randomly shuffling the pixel positions with the key being an array containing $(width * height)$ zero values duplicates. The elements of this array are the result of randomly shuffling the numbers from 1 to $(width * height)$, where $width$ and $height$ are width and height height of watermarked image, respectively.

Step 3: Distribute the scrambled logo using visual cryptography using the (k, n) secret sharing scheme and select a secret share to be watermarked.

Step 4: Perform a DWT-1-level transformation on any color (RGB) channel of the containing image to obtain 4 subbands (LL1 - LH1 - HL1 - HH1).

Step 5: Choose one subband (Here, we choose LL band) and embed watermark with logic based on the method in the paper [24]:

$$S^*_{ij} = \begin{cases} S_{ij} - (S_{ij} \ mod \ Q) + 0.75 * Q, & \text{if } W(i,j) = \text{“1”} \\ S_{ij} - (S_{ij} \ mod \ Q) + 0.25 * Q, & \text{if } W(i,j) = \text{“0”} \end{cases} \tag{1}$$

Given:

- S_{ij} is the value at (i, j) on the sub-band of the original image.

- S^*_{ij} is the value at the corresponding position on the image after embedding the watermark.

- Q is the quantization step.

After embedding the $W(i, j)$ information, the value of S_{ij} will be shifted around the origin of S_{ij} based on the quantum step value Q. The quality of the image after embedding the information will depend on the magnitude of the quantum step value Q. At the same time, the stability of the watermark will also be affected by the quantum step value Q.

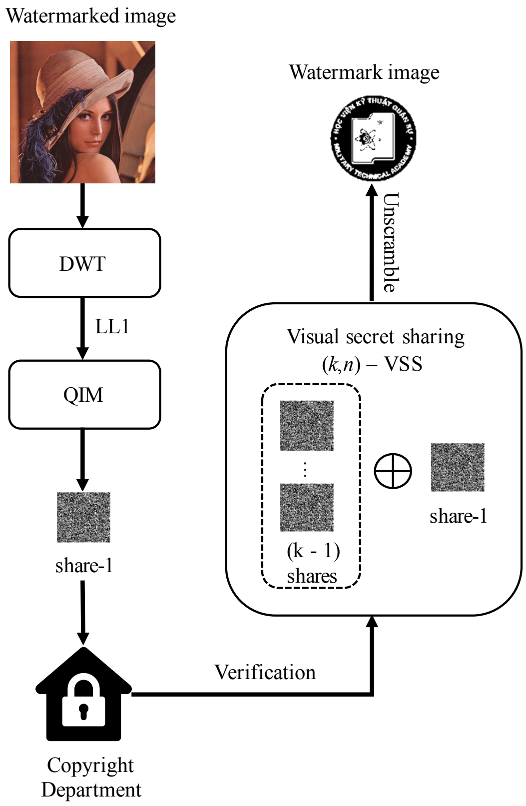


Figure 7. Watermark extraction algorithm combined with VSS

Step 6: Perform Inverse DWT transformation (IDWT) to get image after embedding watermark.

We use the LL subband because after performing the DWT transform, the values of the DWT coefficients carrying the "energy" of the whole image are concentrated mainly in the LL subband. The selection of LL sub-band for information embedding will affect the quality of the image after embedding, but the value domain used for embedding will be richer because the values of non-zero DWT coefficients are mostly concentrated in the sub-band LL [27, 28]. On the other hand, we use QIM embedding algorithm, so the effect of image quality is minimized after embedding information.

2. Watermark extraction algorithm combined with VSS

The input data for the watermark extraction process is the watermarked image, the output of the watermark extraction process is the original watermark image (the logo before being distributed). The watermark extraction process is described in Figure 7.

The watermark extraction process is carried out according to the following steps:

Step 1: *Input:* The watermarked image

Step 2: Perform a discrete wavelet transformation on the watermarked color channel and select subband LL1.

Step 3: Extract the watermark according to the following equation:

$$\text{If } (S^*_{ij} \ mod \ Q) > Q/2 \text{ then } W^*(i,j) = "1",$$
$$\text{If } (S^*_{ij} \ mod \ Q) < Q/2 \text{ then } W^*(i,j) = "0",$$

where:

- S^*_{ij} is the value at position (i,j) on the watermarked subband.

- $W^*(i,j)$ is the value at (i,j) of the extracted watermark.

- Q is the quantization step.

Step 4: Combine the watermark extracted in Step 3 with another $(k-1)$ shared secret fragments to reproduce the logo.

Step 5: Perform unscramble recovery to obtain the complete copyright logo by re-positioning the pixels according to the key generated during the watermark embedding process.

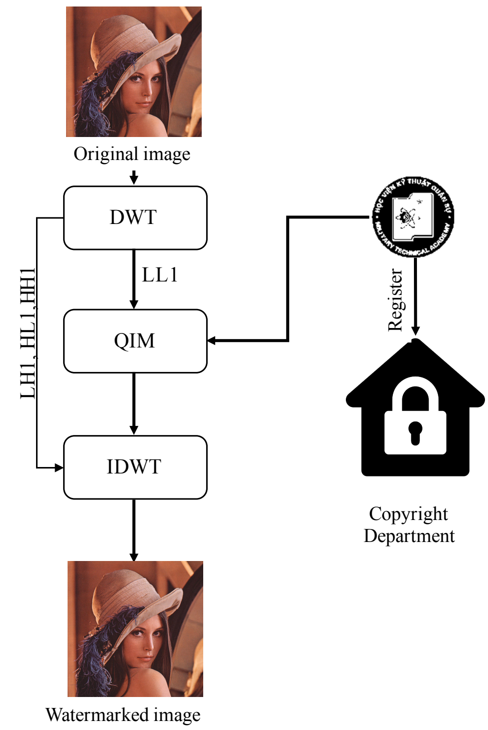


Figure 8. Watermark embedding using only DWT-QIM

3. Watermarking/embedding algorithm using only DWT-QIM

To compare the effectiveness of the proposed solution, we perform a traditional DWT domain watermarking method (called DWT-QIM solution) to evaluate and determine the highlights and feasibility of the method.

a. Watermarking embedding process:

The process of embedding the watermark using only DWT-QIM is described in Figure 8. The process of embedding the watermark is done in the same way as in III.1, but steps 2 and 3 are omitted.

b. Watermark extraction process:

The process of watermark extraction using only DWT-QIM is described in Figure 9. The process of watermark extraction is done in the same way as in III.2, but steps 4 and 5 are omitted to recover the watermark image after extraction.

IV. Experimental results and evaluation

1. Evaluation measure

We conduct experiments and compare the results of two methods: the embedding/watermarking method combining DWT-QIM with visual cryptographic techniques (VSS) and the embedding/watermarking method using only DWT-QIM to compare the effectiveness of our method.

We evaluate the results of the experiments through two properties: "Unrecognizability" represented by the peak signal/noise ratio - PSNR (Peak Signal to Noise Raito) measured in decibel with formula (2) and "Stability" of the watermark after extraction, represented by the value NC (Normalization Correlation) calculated by the formula (4).

$$PSNR = 20\log_{10}\frac{MAX(I)}{\sqrt{MSE}}, \quad (2)$$

where, $MAX(I) = 255$ and the value of MSE is calculated by formula (3):

$$MSE = \frac{1}{p \times q}\sum_{i=1}^{p}\sum_{j=1}^{q}(I(i,j) - I_w(i,j))^2, \quad (3)$$

where $I(i,j), I_w(i,j)$ is the pixel value of the original and watermarked image at position (i,j). The value $p \times q$ is the size of the image.

For PSNR, the higher the value of the PSNR, the more "unrecognizability" is guaranteed. If the value of PSNR $\geq$ is 35dB, the human eye cannot distinguish between the original image and the image that has been watermarked.

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j).W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}, W(i,j)^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}, W'(i,j)^2}}, \quad (4)$$

where, $M_1 \times M_2$ is the size of the logo, $W(i,j), W'(i,j)$ is the value of the elements of the original logo and the restored logo. The cross-correlation coefficient normalizes NC and has a value between 0 and 1. The closer the value

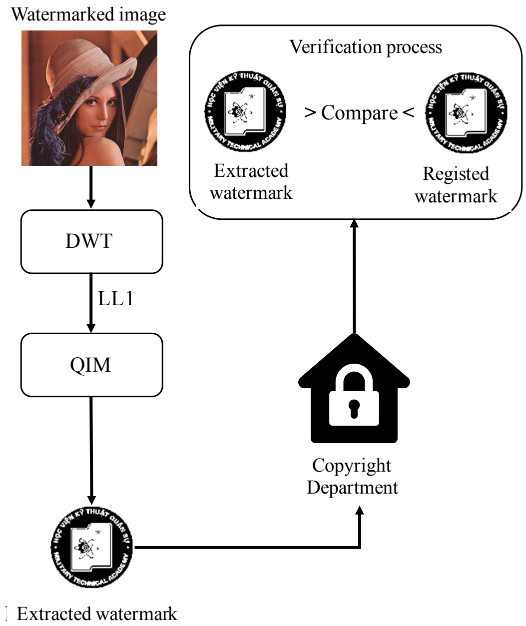


Figure 9. Watermark extraction using only DWT-QIM

of NC is to 1, the better the stability of the watermarking solution. However, NC greater than or equal to 0.75 is an acceptable threshold.

2. Experimental environment

We have built a program to simulate embedding and extracting watermarks using MATLAB R2013a (8.1.0.604)

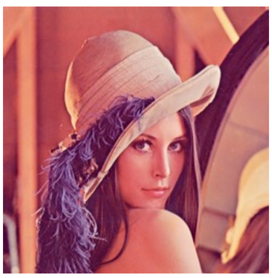


Figure 10. Lena image

Figure 11. Watermark logo

Figure 12. Experimental Lena image when embedding watermark by DWT-QIM method combined with VSS

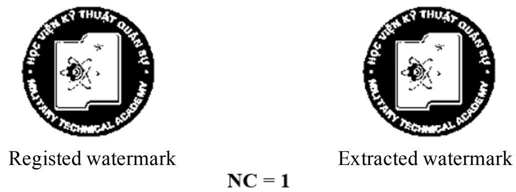


Figure 13. Extraction and reconstruction results of watermark by DWT-QIM method combined with VSS.

- 64bit. The program is installed on Laptop with system parameters such as: Windows 10 Pro operating system, Intel(R) Core(TM) processor i5-8625U CPU @ 1.60GHz 1.80GHz, 8GB RAM.

In this paper, we choose Lena image (Figure 10) as the image to be protected by copyright and a binary image as the copyright logo (Figure 11). We use Haar algorithm for DWT transformation. The parameters used for VSS in the test are $k = 4$ and $n = 10$.

3. Results of watermarking with combined VSS and without combined VSS

a. Experimental results with DWT-QIM method combined with VSS (Proposed Method)

Figure 12 shows the result after watermark embedding using the proposed method.

Figure 13 shows the results of watermark extraction using the proposed method.

b. Experimental results using only DWT-QIM method

Figure 14 shows the results after embedding the watermark when using only the DWT-QIM method (not combining with VSS).

Figure 15 shows the results of watermark extraction when using only DWT-QIM method (not combining with VSS).

4. Determine the value of Q in QIM

In our proposal, the value of Q (Quantization step) plays a decisive role in the two criteria evaluating the efficiency of the algorithm, namely, the "unrecognizability" of the image after watermark embedding is represented by the ratio $PSNR$, and the "sustainability" of the watermark after it is extracted is expressed by the value NC. The smaller Q is, the larger $PSNR$ is and the smaller NC is. This means the smaller Q is, the greater the imperceptibility and the lower the stability of the watermark is.

As stated at the beginning of Section IV, each of the above values has its standard threshold. With a PSNR of 35dB and a NC of 0.75. Therefore, to balance between the above two values when embedding and extracting watermarks, we have tested on different Q values to give the most reasonable value. The values of $PSNR$ and NC with different Q are shown in Table I.

TABLE I
$PSNR$ AND NC VALUE WITH DIFFERENT Q

Quantization step (Q)	NC	$PSNR$ (dB)
5	0.75	48.09
10	1	42.72
15	1	39.02
20	**1**	**36.57**
25	1	34.59
30	1	32.97

Accordingly, we decided to choose the quantization step $Q = 20$ for our proposal because there the values of $PSNR$ and NC are closest to the standard level.

5. Image quality evaluation

To evaluate the image quality after watermarking of the proposed method, we use a dataset of 05 images: Lena, Pepper, Couple, Mandrill and Parrots with size 512×512 and choose 01 binary logo size 64×64 to be our copyright logo. Simultaneously, the experiment was conducted with both methods: the proposed method (DWT-QIM-VSS) and

Original image Watermarked image
PSNR = 42.2562

Figure 14. Watermark embedding results in DWT-QIM method

Registed watermark Extracted watermark
NC = 0.99861

Figure 15. Watermark extraction results when using only DWT-QIM method

the conventional watermarking method (DWT-QIM) on the Blue channel of the test image to compare the rating results. The results are shown in Figure 16 and Table II.

With the obtained results, we find that using the proposed watermarking method gives better $PSNR$ results than using the conventional method.

6. Robustness evaluation

As mentioned above, the value NC represents the stability of the watermark after it is extracted. In this section, we conduct tests and comparisons with watermarked images using both methods: using only DWT-QIM based on the idea of [25, 26] and DWT-QIM watermarking method combines VSS (recommended method) in the condition of being unaffected and affected by common attacks. Next, we extract the watermark and calculate the NC value to evaluate the sustainability of the watermark under the above conditions.

a. Watermark extraction results when not affected by attack spells

The results of watermark extraction on the dataset of 05 images: Lena, Pepper, Couple, Mandrill, Parrots, in the unattacked condition when using 2 different watermarking methods to embed the watermark are shown in Figure 17 and Table III. From the results of this experiment, we can see that the proposed method has better results even when the watermarked image has not been attacked by any image attacks.

b. Watermark extraction results under the influence of normal attacks

TABLE II
PSNR IN THE TRADITIONAL WATERMARK METHOD AND THE PROPOSED METHOD.

Image	PSNR (DWT-QIM)	PSNR (DWT-QIM & VSS)
Lena	36.3811	36.5217
Pepper	36.3224	36.4191
Couple	36.2893	36.6512
Mandrill	36.3538	36.5417
Parrots	36.5033	36.7141

Figure 16. Test results of 2 watermarking methods with a dataset of 05 images

TABLE III
NC VALUES IN UNATTACKED CONDITION

Image	NC (DWT-QIM)	NC (DWT-QIM & VSS)
Lena	0.997711	1
Pepper	1	1
Couple	0.999852	0.999481
Mandrill	0.999718	1
Parrots	0.995578	0.999574

TABLE IV
VALUE OF NC WHEN THE WATERMARKED IMAGE IS AFFECTED BY ATTACKS.

Type of attacks	NC (DWT-QIM)	NC (DWT-QIM & VSS)
Gaussian noise (0.01)	0.27106	0.75892
Poisson noise	0.262291	0.756114
Salt & Peper (0.02)	0.977128	0.983195
JPEG (QF = 50)	0.309221	0.787013
Histogram Equalization	0.394625	0.786501
Median filter (3 × 3)	0.833469	0.842374
Laplacian Sharpening	0.26666	0.777764
Blur (3 × 3)	0.272942	0.760467

Figure 18 and Table IV show the visual results as well as concrete data when extracting watermark from container image using different methods for watermark embedding under conditions affected by normal attacks. The reason our proposed solution has a better result than the DWT-QIM algorithm is because of the following reasons: In the DWT-QIM solution combining VSS, we disperse the original watermark into n. fragment and use only 1 fragment to embed information like DWT-QIM solution. However, because the remaining $(n-1)$ fragment is used to register with the Copyright Office, when extracting information a watermark fragment from the watermark image is attacked and restored with $(k-1)$ fragment taken from $(n-1)$ piece stored by Copyright Office will recover watermark information close to original watermark. Thereby proving the copyright even though the watermarked image has been attacked to change the image. This point is the difference of the proposed algorithm combining encryption and watermarking to secure watermark information and strengthen its stability against some common attacks. Thus, the experimental results show that the proposed solution is effective in copyright protection on digital images.

c. Proving DWTT-QIM-VSS is more sustainable than DWT-QIM

To prove the stability of the proposed solution, DWT-QIM-VSS, with the method using only DWT-QIM, we assume that the watermark images of both methods are attacked by any image attack. Then, the DWT-QIM method extracts the watermark image W', the DWT-QIM method & VSS extracts the watermark image S_1', with $S_1, S_2, \cdots, S_n$

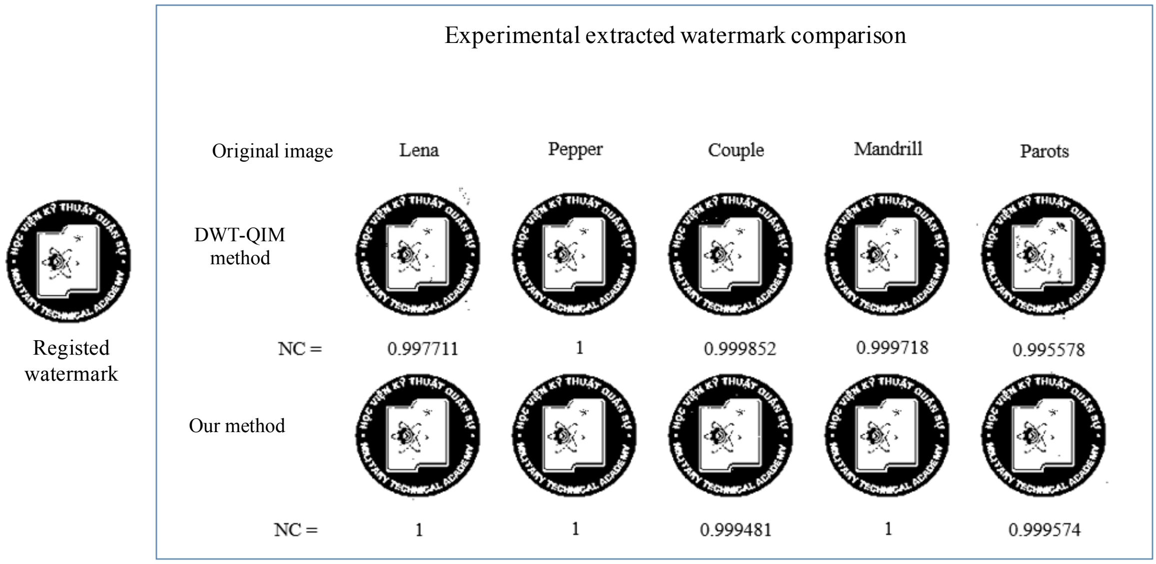


Figure 17. Result of watermark extraction in unattacked condition

is n shared fragment generated in VSS algorithm in II.1 and S_1' is watermark extracted from hacked image of watermark S_1. Without loss of generality, we assume that the change of W' relative to W and the change of S_1' relative to S_1 are the same. Use VSS to recover watermark W'' according to the following formula:

$$W'' = S_1' \ OR \ S_2 \ OR ... OR \ S_n, \quad (5)$$

We need to prove $NC(W, W'') > NC(W, W')$.

Proof: Assume the same variation for W' and S_1', ie:

Assume the same variation for W' and S_1', ie:

$$TS(W, W') = TS(S_1, S_1') = P > 0, \quad (6)$$

where, $TS(W, W')$ is the sum of the errors between W and W', and $TS(S_1, S_1')$ is the sum of the errors between S_1 and S_1'.

Set

$$Z_0 = \{(i, j)|W(i, j) = 0\}, Z_1 = \{(i, j)|W(i, j) = \text{“1”}\} \quad (7)$$

Then, according to the properties of VSS, we have:

$$S_1(i, j) = 0, \forall(i, j) \in Z_0 \quad (8)$$

Assume the error is evenly divided by Z_0 and Z_1. That means if the notation X_0 is the set of errors over Z_0, X_1 is the set of errors over Z_1 of W' and Y_0 is the set of errors over Z_0, Y_1 is the error set on Z_1 of S_1', then:

$$Sp(X_0) = Sp(X_1) = Sp(Y_0) = Sp(Y_1) = \frac{1}{2}P, \quad (9)$$

where $Sp(U)$ is the number of elements of the set U.

According to the properties of VSS (assuming $2 \leq k < n$):

$$\forall(i, j) \in Z_0 \implies S_t(i, j) = 0, t = 2, ..., n$$
$$\forall(i, j) \in Z_1 \implies S_2(i, j) \ OR \ ... \ OR \ S_n(i, j) = 1, t = 2, ..., n$$

From that and (5), (7), (8) deduce:

$W''(i, j) = 1, \forall(i, j) \in Z_1$ (false fixed on Z_1)

$W''(i, j) = 0, \forall(i, j) \in Z_0, Y_0$

$W''(i, j) = 1, \forall(i, j) \in Y_1$ (cannot be corrected on Z_0)

Contrast this with (7), we get:

$$TS(W, W'') = Sp(Y_0) = \frac{1}{2}P \quad (10)$$

Combine this formula with (6), and get:

$$TS(W, W'') = \frac{1}{2}TS(W, W') \quad (11)$$

Thus, the error of W'' is halved compared to W'.

Now if we put: $T = Sp(Z_1), q = Sp(X_0) = Sp(X_1) = Sp(Y_0)$, it's easy to see:

Above Z_1: W and W'' both have T pixels equal to "1"; W' only $(T - q)$ pixels equals "1".

Above Z_0: W has $Sp(Z_0)$ pixels equal to "0"; W' and W'' have $Sp(Z_0) - q$ pixels equal to "0".

From there it is easy to calculate:

$$\begin{aligned} NC(W, W'') &= \frac{T}{\sqrt{T}\sqrt{T + q}} \\ NC(W, W') &= \frac{T - q}{\sqrt{T}\sqrt{T}} \end{aligned} \quad (12)$$

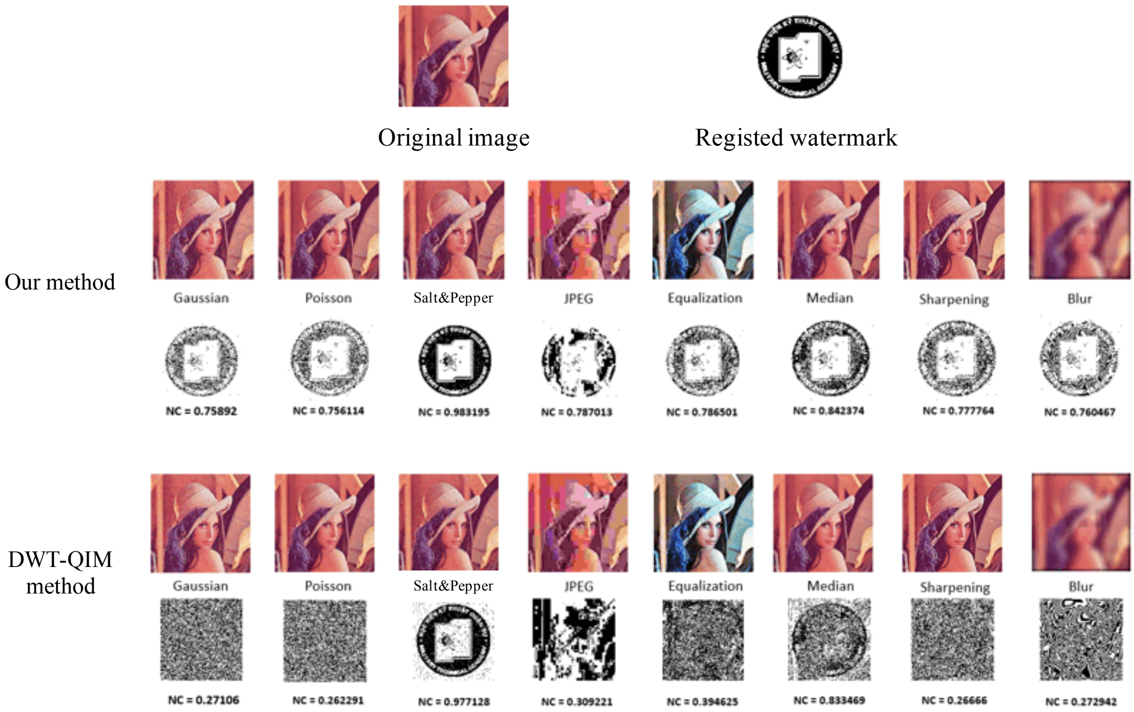


Figure 18. Watermark extraction results under many attacks

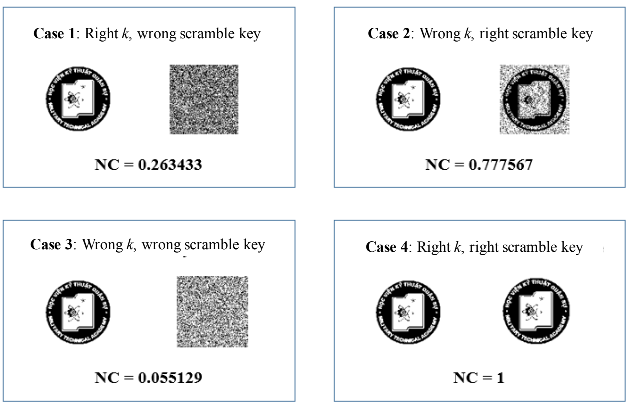


Figure 19. Copyright logo is reproduced in different cases

Thus, to prove that $NC(W, W'') > NC(W, W')$, it is necessary to show:

$$\frac{T}{\sqrt{T+q}} > \frac{T-q}{\sqrt{T}} \tag{13}$$

This is equivalent to:

$$T\sqrt{T} > (T-q)\sqrt{T+q}$$

Square both sides:

$$T^2 T > (T-q)^2 (T+q) = (T^2 - q^2)(T-q)$$

This is obviously true, so the proof is complete.

Thus, with the condition that it is not affected by normal attacks, the value of NC between the original watermark and the extracted watermark when using both methods is relatively similar. It is difficult to conclude that our proposed watermarking method is more stable than the method using only DWT-QIM in this condition. Therefore, we conduct experiments with conventional image attacks on images containing Lena watermark to once again evaluate the effectiveness of the algorithm. The results show that the proposed method of watermarking using DWT-QIM in combination with VSS can ensure the stability of the watermark against common attacks.

7. Security evaluation

In this paper, to enhance the security of the copyright logo, in addition to the visual cryptographic technique (VSS), we also use the scramble technique on the copyright logo before distributing it into n shared secret fragments. We use Arnold Transform [29] and shuffle key = 10 to shuffle the logo image before scattering using VSS. Thus, to restore the copyright logo, it is necessary to have 02 elements, namely: “Minimal share k value to restore copyright logo” and “key scramble” to recover scramble.

In this section, we evaluate the security of the algorithm against copyright information in the cases shown in Figure 19 and Table V.

TABLE V
NC VALUES FOR EACH KEY

Test case	NC
Right k, wrong scramble key	0.263433
Wrong k, right scramble key	0.777567
Wrong both k và scramble key	0.055129
Right both k và scramble key	1

Thus, through tests in each specific case, we have shown that the algorithm we propose can completely secure the information of the copyright logo.

V. Conclusion

Our paper proposes a digital image copyright protection solution based on the method of combining digital watermarking with visual cryptography to create a more sustainable and effective method in the digital image protection and digital product copyright.

From the results obtained through various tests with both the algorithm when using DWT-QIM in combination with VSS (recommended method) and using only DWT-QIM, we found that when using only DWT-QIM, the image quality after watermark embedding is worse than that of the proposed method. However, with tests under the influence of attacks, using the proposed method will ensure more robustness of the watermark than the traditional method of using only DWT-QIM.

Thus, in this paper, we have shown that: with the application of visual cryptographic techniques to disperse watermarks, and at the same time combine the watermarking algorithm based on the discrete wavelet transform DWT using DWT. quantization index (QIM), has contributed to improving the imperceptibility as well as the stability of the watermark against conventional attacks.

Acknowledgment

This research is funded by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.01-2019.12

References

[1] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 30523–30533, 2019.

[2] M. Charfeddine, M. El'arbi, and C. B. Amar, " A new DCT audio watermarking scheme based on preliminary MP3 study," *Multimedia Tools Appl*, vol. 70, no. 3, pp. 1521–1557, 2014. DOI:https://doi.org/10.1007/s11042-012-1167-0

[3] Roy, S., & Pal, A. K., "An indirect watermark hiding in discrete cosine transform-singular value decomposition domain for copyright protection," *Royal Society open science*, 4(6), 2017. https://doi.org/10.1098/rsos.170326

[4] Barni M., Bartolini F., Piva, A., "Improved wavelet-based watermarking through pixel-wise masking," *IEEE transactions on image processing*, 10(5), pp.783–791, 2001.

[5] Singh A. K., Kumar B., Dave M., Mohan A., "Robust and imperceptible dual watermarking for telemedicine applications," *Wireless Personal Communications*, 80(4), pp. 1415–1433, 2015.

[6] Singh A. K., Dave M., Mohan A.," Robust and secure multiple watermarking in wavelet domain," *Journal of medical imaging and health informatics*, 5(2), pp. 406–414, 2015.

[7] Singh AK, Dave M, Mohan A, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools Appl*:121, 2015.

[8] Urvoy M., Goudia D., Autrusseau F., "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions," *IEEE Transactions on Information Forensics and Security*, 9(7), pp. 1108–1119, 2014.

[9] Cedillo-Hernandez M., Garcia-Ugalde F., Nakano-Miyatake M., Perez-Meana H., "Robust digital image watermarking using interest points and DFT domain," In: 35th *IEEE International Conference on Telecommunications and Signal Processing (TSP)*, pp. 715–719, 2014.

[10] T. M. Thanh, K. Tanaka, "The novel and robust watermarking method based on q-logarithm frequency domain," *Multimedia Tools and Applications*, volume 75, pp. 11097–11125, 2016.

[11] T. M. Thanh, K. Tanaka,"A proposal of novel q-DWT for blind and robust image watermarking," *Proceeding of IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Washington D.C., pp. 2066–2070, 2014.

[12] T. M. Thanh, P. T. Hiep, T. M. Tam, "A New Spatial q-log Domain for Image Watermarking," *IJIIP: International Journal of Intelligent Information Processing*, Vol. 5, No. 1, pp.12–20, ISSN 2093-1964, 2014.

[13] T. M. Thanh, K. Tanaka, "An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information," *International Journal of Multimedia Tools and Applications (MTAP)*, ISSN: pp. 1573–7721, 2016.

[14] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D. et al. "Digital watermarking techniques for image security: a review," *J Ambient Intell Human Comput* 11, pp.3221–3229 (2020).

[15] M. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptology (EUROCRYPTO 94)*, (Lecture Notes in Computer Science), vol. 950, A. De Santis, Ed. Berlin, Germany: Springer-Verlag, pp. 1–12, 1995.

[16] A. Shamir: "How to share a secret ?" Comm ACM, 22(11): pp. 612–613, 1979.

[17] Mukesh Dalal, Mamta Juneja , "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," *International Journal of Multimedia Tools and Applications (MTAP)*, ISSN: 80, pp. 5723—5771, 2021.

[18] G. Blakley, "Safeguarding cryptographic keys," *Proc. of AFIPS National Computer Conference*, 1979.

[19] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE transaction on Information Theory*, 29(2), pp. 208–210, 1983.

[20] Shyamalendu Kandar and Bibhas Chandra Dhara, "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence," *International Journal of Computer Applications* (0975 – 8887), Volume 25, No.11, July 2011.

[21] E. Elbasi, A. M. Eskicioglu, "Naïve Bayes Classifier Based Watermark Detection in Wavelet Transform," *Multimedia Content Representation, Classification and Security (MRCS)*, Lecture Notes in Computer Science, vol 4105, 2006.

[22] S. Huang, W. Zang, "Blind Watermarking Scheme Based

on Neural Network," *The 7th World Congress on Intelligent Control and Automation*, Chongqing, pp. 5985–5989, 2008.

[23] Giang Ngọc Dân, Tạ Minh Thanh, "Giải pháp bảo vệ bản quyền ảnh số dựa trên kỹ thuật kết hợp thủy vân số và mã hóa trực quan," *Journal of Science and Technology on Information and Communications*, 2020.

[24] R. Sun, H. Sun, T. Yao, "A SVD and Quantization Based Semi_fragile Watermarking Technique for Image Authentication," *ICSP'02 Proceedings*, pp. 1592–1595, 2002.

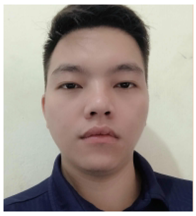
[25] A. Akter, Nur-E-Tajnina, M. A. Ullah, "Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm," *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, 2014, pp. 1–6, doi: 10.1109/ICIEV.2014.6850699.

[26] A. Benoraira, K. Benmahammed, N. Boucenna, "Blind image watermarking technique based on differential embedding in DWT and DCT domains," *EURASIP Journal on Advances in Signal Processing*, vol 55, 2015.

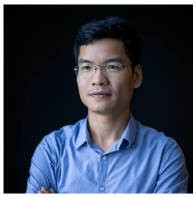
[27] O.Jane, E. Elbasi, H.G.Ilk, "Hybrid Non-Blind Watermarking Based on DWT and SVD," *Journal of Applied Research and Technology*, vol. 12, Issue 4, pp. 750–761, 2014.

[28] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, Talal Shamoon. "Secure spread spectrum watermarking for multimedia," *IEEE transactions on image processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[29] M. Li, T. Liang, Y. He, "Arnold Transform Based Image Scrambling Method," *3rd International Conference on Multimedia Technology*, pp. 1309–1316, 2013.



Dan Giang Ngoc is currently studying Network Technology at Le Quy Don University. His field of research is digital watermarking for digital multimedia.
Email: giangngocdan3110@gmail.com.



Thanh Ta Minh is currently an associate professor and vice dean of Faculty of Information Technology in Le Quy Don Technical University Vietnam. He is also a Postdoctoral Fellow of the Department of Mathematical and Computing Sciences at Tokyo Institute of Technology. He received his B.S. and M.S in Computer Science from National Defense Academy, Japan, in 2005 and 2008 and his Ph.D. from Tokyo Institute of Technology, Japan, in 2015, respectively. He is the member of IPSJ Japan and IEEE. His research interests lie in the area of watermarking, network security, and computer vision.
Email: thanhtm@lqdtu.edu.vn.