Check for updates

Pseudo Zero-Watermarking Algorithm Using Combination of Non-blind Watermarking and Visual Secret Sharing Scheme

Le Danh Tai[1,2], Cao Thi Luyen[1,2], and Ta Minh Thanh[1,2(✉)]

[1] Le Quy Don Technical University, 236 Hoang Quoc Viet, Hanoi, Vietnam
thanhtm@lqdtu.edu.vn
[2] University of Transport and Communications, Hanoi, Vietnam
http://fit.mta.edu.vn/

Abstract. This paper proposes a solution for digital image copyright protection technique using the combination of watermarking and visual encryption technique. In our solution, the copyright information (copyright logo) is distributed into n shares using $k - out - of - n$ distributed algorithm, also called (k, n) visual secret sharing method. One of the shares is randomly selected to embed into the original image to prove the user's copyright. The remaining $n - 1$ shares is used to register with Copyright Department. When claiming the copyright belongs to the user, the verifier only needs to extract the watermark information from the watermarked image, then decodes with any registered $k - 1$ shares from $n - 1$ shares for restoring copyright information. Experimental results of the proposed method compared with the method using only digital watermark show that our method has more practical effectiveness in the application of digital product copyright protection.

Keywords: Digital watermarking · Visual secret sharing - VSS · Copyright protection · Discrete Wavelet Transform (DWT) · Discrete Cosine Transform (DCT) · Copyright authority

1 Introduction

1.1 Overview

The number of digital contents delivered over the Internet has been increased in recent years. According to the development of network technologies, the unauthorized copies and manipulation of digital contents have become a serious problem. It also raised the problems of infringing on copyright and affecting the interests of the digital content creators. In order to solve such problems, a lot of watermarking methods have been proposed for protecting the author's copyright. The watermarking algorithms can be applied on the spatial domain and the frequency

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2021
Published by Springer Nature Switzerland AG 2021. All Rights Reserved
N.-S. Vo et al. (Eds.): INISCOM 2021, LNICST 379, pp. 448–464, 2021.
https://doi.org/10.1007/978-3-030-77424-0_36

domain. In general, the watermarking methods used frequency domain are more robust than that of methods used spatial domain.

In the previous watermarking methods, some frequency domains are suitable for robust watermarking methods such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT). The frequency domain based robust watermarking methods have been shown in recently *e.g.* DCT-based [1–4], DWT-based [5–8], and DFT-based [9,10]. These methods had proved that the frequency domain is efficient for digital right management system. In general, when we embed directly the watermark information into the digital image, its quality may be degraded. Also, the watermark information cannot be extracted when the embedded images are modified under some attacks such as image processing and geometrical processing.

In order to achieve the balance of better quality of the watermarked images and the robustness of watermark extraction, some improved frequency domains are proposed such as q-DCT [11], q-DWT [12], and q-SVD [13]. According to the values of q parameter, those proposed methods could provide a new frequency domain for such purpose. However, the optimization of the values for q parameter is quite complicated, then it depends on many experiments and those of analysis.

With an another approach, the zero-watermarking methods, in which the watermark information is not embedded into the digital contents, are frequently proposed for digital contents [14]. The zero-watermarking methods are mainly employed the robust feature of the content in order to encode with the watermark information, the generate the master share (MS) and the owner share (OS). The MS is used to register to Copyright Office. When the dispute occurs, the feature of the contents is extracted again, then decodes with the owner share to generate the watermark. According to the visual of watermark information, the copyright authority can judge the ownership of the digital contents. However, the drawback of zero-watermarking is to depend on a lot of features extracted from the digital contents. That may be affected when the digital contents are degraded under strong attacks.

The concept of joint visual cryptography and watermarking method [18] is proposed to take a balance of the robustness and the visual quality. In this system, the watermark can only be achieved if all of the shared images are collected. In the other hand, the watermarking method usually embed the watermark information into the digital image its self while preserving the quality of the watermarked image. Based on those merits, the joint visual cryptography and watermarking method proposes a new approach for digital copyright protection.

1.2 Our Contributions

We summarise our contributions in this paper as follows.

We propose a new embedding method utilizing both frequency domain based embedding approach and VSS in order to reduce the amount of watermarking information that is embedded into the digital contents itself. Since our proposed method employs the color watermark image as copyright information, the embedded amount of watermark information should be considered to improve

the quality of watermarked contents while remaining the meaning of copyright protection solutions. In our proposed method, the color watermark information is encoded by AES (Advanced Encryption Standard) encryption [27], then created n shares to generate OS and MS by using (k, n) visual secret sharing method. One of the shares, *e.g.* OS, is randomly selected to embed into the original image to prove the user's copyright. Other shares are used as MS to register for Copyright Office. According to our method, the number of watermark bits embedded into the copyrighted contents is litter compared to that of conventional watermarking methods.

In our understanding, in order to achieve the robustness of watermarking method, we need to propose the methods that let not the hackers can break or destroy the watermark information from the watermarked contents. Therefore, our proposed method does not depend on the feature of digital contents, which may be the clues for hackers try to destroy the contents either the watermark information. Since our method uses random one of share as the watermark information for embedding into the DWT frequency domain, it certainly reduces the dependent of the feature of digital contents like zero-watermarking methods. However, our extracted watermarking information can be decoded with MS (remain of $k-1$ shares) to confirm the registered copyright information.

We also employ AES encryption to encode the color watermark information. After that, we apply (k, n)-VSS method on the encoded color watermark information to separate n shares using in our system. Only the person who has AES key and secret key (k, n) can decode the watermark information and verify the copyright of digital contents. That makes our proposed method more secure comparing with previous zero-watermarking methods.

1.3 Roadmap

This paper is organized as follows. Section 2 gives surveys of related works. Section 3 introduces our proposed pseudo zero-watermarking technique based on non-blind Watermarking and VSS for color images and color watermark image. Section 4 presents the results of the experiments and Sect. 5 concludes our paper.

2 Related Works

There are many image watermarking algorithms using VSS for copyright protection. However, they are tended to follow the same patterns and processed steps to ensure the security of cover image. According to the our survey, we describe the general algorithm of these methods. Then, we also explain the different entities of the integrated system and each role of them.

In general, most of zero-watermarking techniques are proposed based on VSS (*e.g.* visual cryptography - VC) for spatial domain. We call it VZWS. The concept of VSS using in the zero-watermarking is described in paper [19,20]. VC is employed as an extended VSS algorithm for protecting the digital images. Such problem of VC is shown as the special case of a $2-out-of-2$ visual

secret sharing problem. The secret image is divided into two shares that consist of random dots of the secret images by using the corresponding location of each pixel from secret image. In order to decode the secret image, the secret image can be easily detected when these shares are stacked together.

Firstly, Hwang [28] had built up an zero-watermarking method based on the concept of VC. In his method, the secret information (watermark information) is not embedded directly into the original image. Hwang's method makes it harder to detect/recover from the watermarked image. The watermark information can be obtained by stacking all shares together, without making comparison with the original image. However, since Hwang's method extracts the LSBs (Least Significant Bit) for XOR-ing with the watermark pattern, then its algorithm may not secure and be robust against various strong attacks.

In order to enhance the security of the method [28], Surekha *et al.* [32] proposed a similar MSB (Most Significant Bit) based algorithm in which a XOR operation is involved for encryption with watermark logo. It achieved better security than that of Hwang, but it could not improve the robustness. Also, Surekha *et al.* employed the feature of MSBs for encoding, therefore, it increases the probability of false positive. Also, since the increasing of false positive, it leads to ambiguity in authority verification when the depute happens. Hence, such algorithms cannot be applied for copyright protection.

In another approach, Bolla *et al.* [30] proposed a method by using the statistical properties of sampling distribution of means (SDM) to improve the required security that is mentioned above. This method used the SDM features from original image to create the master share (MS). After that, MS is employed together with the watermark pattern for generating the information of ownership share (OS) using VC(2,2) with a block of 4 subpixels. The results of this method that can resist several processing attacks and geometric attacks.

Since VZWS methods almost employ the spatial feature involving with the watermark pattern, the security issues are not ensured enough. There are some papers focused on proposal of frequency based feature to attain the security and to improve the robustness of their method. We call it VZWF.

In the paper of Wang *et al.* [31], they proposed a watermarking method that extracts the feature of SVD (Singular Value Decomposition) domain to encode with watermark information in order to improve the security and robustness. In their method, the random 31×31 blocks are selected. After that, the SVD is applied to each block, then the singular value (SVs) is selected to generate the MS. The security of their method is improved by using decomposition into random several blocks, and using a variant of the VC (2,2) with a block of 4 sub-pixels. Based on such approach, the OS is generated. In order to confirm the authority rights, the MS is constructed with the same process, and then superimposed on the OS to extract the watermark. Wang's method focused on using the feature of frequency domain based on the secret key for randomizing the blocks patterns.

To solve the false positive problem (FPP), Surekha *et al.* [32] proposed a watermarking method using the feature of DWT (Discrete Wavelet Transform)

domain. It presented a new VC(2,2) scheme called Pair-Wise Visual Cryptography (PWVC) which measures the security criteria for ensuring the reliability of the method. Also, they used PWVC to avoid the distortion of the watermark information by creating shares with same size as the original watermark. In their method, the LL sub-band of DWT domain is randomly selected by using secret key to reconstruct the feature matrix which contains the averages of selected blocks. According to the feature matrix, the MS is generated by using PWVC algorithm. In order to confirm the authority rights, the same process is repeated to generate the MS, the latter is superimposed on the OS to extract the watermark.

In order to improve more securely, Thanh *et al.* [14] proposed a new image zero-watermarking algorithm based on the encryption of visual map feature (VMF) or permuted visual map feature (PVMF) extractes form original image with copyright information. They employed the robust feature extracted from the cover image by taking the combination of QR decomposition and 1D-DCT. Then, they encrypted the VMF and PVMF feature with the watermark information to generate MS and OS. Therefore, they could improve the security of method by randomizing visual feature of original images. They had demonstrated that their method is robust against common processing and geometric attacks, also it is with low consuming time.

3 Our Pseudo Zero-Watermarking Technique Based on Non-blind Watermarking and VSS

According to above analytic, we found that the mentioned issues can be solved by improving VSS and watermarking technique. This section explains the detail our proposed method.

3.1 Random Bit Sequence Based (k, n)-VSS Scheme

The (k, n)-VSS scheme provides a method where a secret image is separated into n shares. In this scheme, any k or more shares can generate the secret image by stacking them. However, fewer than k shares get nothing about the secret image.

In general, in secret sharing scheme, there exist n users $U = \{U_1, U_2, ..., U_n\}$ and a provider P. A (k, n)-VSS scheme consists of two phases as follows:

(1) *Sharing phase*: the provider P divides the secret image W into n shares $S_1, S_2, ..., S_n$ and sends each share S_i to a user U_i.

(2) *Reconstruction phase*: a group of at least k users collect and submit their shares to reconstruct the secret image.

Based on the *Sharing phase* and *Reconstruction phase*, the information secret sharing method among many users is established. In order to control the security of secret image W for applying on copyright protection solution, we improve the (k, n)-VSS scheme by using random bit sequence. The detail steps are described as follows:

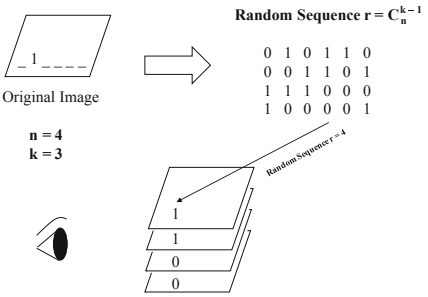

Fig. 1. An illustration of our sharing algorithm.

1. *Sharing algorithm*
   (a) To define the number of shares, the secret key ns is computed by following formula.
   $$ns = C_n^{k-1} \tag{1}$$
   Based on the value of ns, the random bit sequence $\{Sq_1, Sq_2, \cdots, Sq_{ns}\}$ is generated.
   (b) Suppose that the secret image W is divided into n shares $S_1, S_2, ..., S_n$. Such n shares are generated by using our simple algorithm,
      i. All pixels of S_t is set "0" by default values where $(1 \leq t \leq n)$.
      ii. If the value of i^{th} bit of each pixel from the image W is "1", the random value r is generated so that it is between 1 and ns. The corresponding i^{th} bit of S_t is calculated by $S_t(i) = S_j(i)|Sq_r(j)$, where $|$ is OR bit operation, and $1 \leq j \leq n, 1 \leq r \leq ns$. The concept of sharing algorithm is shown in Fig. 1.
2. *Reconstruction phase*
   (a) In order to reconstruct the secret image W, s shares $(k \leq s \leq n)$ are collected. The value of s is randomly created for each reconstruction.
   (b) The secret image W' can be reconstructed by taking the OR operation of all corresponding bit position of each share.
   $$W'(j) = S_1(j)|S_2(j)|...|S_s(j), \tag{2}$$
   where $1 \leq j \leq w \times h$, and $w \times h$ is the size of W.

3.2 Our Pseudo Zero-Watermarking Method

The concept of our pseudo zero-watermarking method is shown in Fig. 2. Our method is composed of watermarking technique and $(k-n)$-VSS technique. The detail steps of our method is described as follows:

1. The color watermark image W is firstly encrypted by using AES algorithm [27] in order to enhance the security of our method. Then, the encrypted watermark image is divided into n shares called $S_1, S2, ..., S_n$ by using (k, n)-VSS method explained in Sect. 3.1.

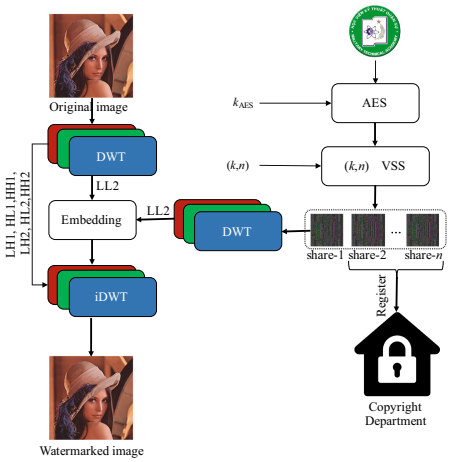

Fig. 2. Our embedding algorithm.

2. A random share is chosen to embed into the original image. For simply, we choose S_1 as the watermark information for watermarking method. The remains ($e.g.$ $S_2, S_3, ..., S_n$) are registered as ownership share (OS) for the office of copyright authority (CA) in order to check the copyright of content.
3. Perform the first-level DWT (applied on RGB component) of the input image I and the share image S_1. Then, the LL_1 sub-band of I and S_1 is performed the second-level DWT. The LL_2 sub-band of I and S_1 is achieved to embed the watermark information.
4. The LL_2 sub-band of S_1 is $S_1^w(i,j)$ is embedded into the LL_2 sub-band of I as follows:
$$LL_2'(i,j) = LL_2(i,j) + \alpha S_1^w(i,j), \tag{3}$$
where α is the strength embedding factor.
5. After embedding the watermark information, the embedded sub-band LL_2' is composed with another sub-bands to perform the inverse DWT (iDWT) and generate the watermarked image I'.

3.3 Copyright Confirmation

Note that, in our method, the master share (MS) is the watermark extracted from the embedded image I'. In order to extract the watermark S_1', the original image I and the watermarked image I' are required. Therefore, our method is non-blind algorithm. However, since our method is used to register with CA for copyright confirmation, so that it is useful in real applications.

If the property dispute concerning the image I' happens. The CA department needs to judge the rightful owner of the such image. The CA asks the owner to provide the secret key such as α, the key k_{AES} of AES encryption, the key (k,n) of (k,n)-VSS, and the secret key ns.

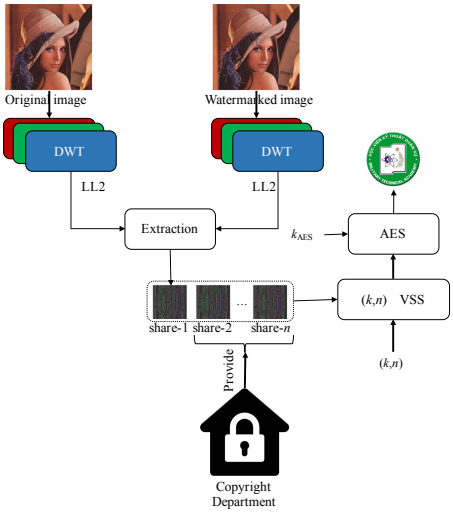

Fig. 3. Our extraction algorithm.

The MS is extracted from the watermarked image by workflow shown in Fig. 3. The explanation is shown as follows:

1. Perform the second-level DWT (applied on RGB component) of the input image I and the watermarked image I'. Then, the LL_2 sub-band of I and I' are retrieved to extract the watermark information ${S'_1}^w(i,j)$, called MS, by using the following formula.

$$ {S'_1}^w(i,j) = (LL'_2(i,j) - LL_2(i,j))/\alpha \tag{4} $$

2. The extracted ${S'_1}^w$ is composed with the remains ($e.g.$ $S_2, S_3, ..., S_n$), called OS. A group of ns shares are used to decoded in (k,n)-VSS scheme, then obtain the AES encrypted image.
3. Finally, the AES encrypted image is decrypted using AES with the secret key k_{AES} to extract the copyright image W'.

According to the extracted image W', CA can judge the rightful owner of the suspected image.

3.4 The DWT-only Method

To justify the utility of combining DWT-based watermark technique with (k,n)-VSS, we propose here a reduced version of our method based only on the DWT domain. That means after encoding the watermark image by using AES encryption with secret key k_{AES}, the encrypted watermark image is performed the second-level DWT on RGB components. Note that, the (k,n)-VSS scheme is

not applied on the DWT-only method. The embedding process is treated with same methodology of Eq. (3).

In the extraction phase, the original image I and the watermarked image I' also are required. The extraction process is treated based on the Eq. (4). The extracted watermark image is again decrypted by using AES encryption with secret key k_{AES} to obtain the watermark information.

According to the extracted image W', CA also can judge the rightful owner of the suspected image.

4 Experimental Results

4.1 Test Images and Evaluation Measures

To perform the efficiency of the proposed method, we conduct five color images of the well known Standard Image Data-BAse (SIDBA) database[1]. The size of our test images are $W \times H = 256 \times 256$ pixels.

To evaluate the quality of experimental images, we use $PSNR$ (Peak Signal to Noise Ratio) criterion [14]. The value of $PSNR$ of $W \times H$ pixels image of $I(i,j)$ and $I'(i,j)$ is calculated as follows:

$$PSNR = 20 \log_{10} \frac{MAX(I)}{\sqrt{MSE}}, \tag{5}$$

where $MAX(I) = 255$ and MSE (Mean Square Error) is calculated as follows:

$$MSE = \sqrt{\frac{1}{W \times H} \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} (I(i,j) - I'(i,j))^2} \tag{6}$$

To verify the robustness of watermark information, we employ the normalized correlation (NC) value between the original watermark W and the extracted watermark W' [14]. The NC value is calculated as follows:

$$NC = \frac{\sum_{i=0}^{L} \sum_{j=0}^{L} W(i,j).W'(i,j)}{\sum_{i=0}^{L} \sum_{j=0}^{L}, W(i,j)^2}, \tag{7}$$

where $L \times L$ is the size of W.

In the experiments, the $PSNR$ value for each attacked image and the NC value for each watermark extracted from the attacked images is calculated. In general, if the $PSNR$ value is larger than 35 dB, the quality of the attacked image is considered to be close to the original image. When the NC value is close to "1", it denotes that the proposed method is robust against the attacks.

To define the suitable value of watermark strength factor, we used the same method of paper [35]. In the rest of our experiments, we set $\alpha = 0.2$ as the default watermark strength factor value.

[1] http://decsai.ugr.es/cvg/index2.php.

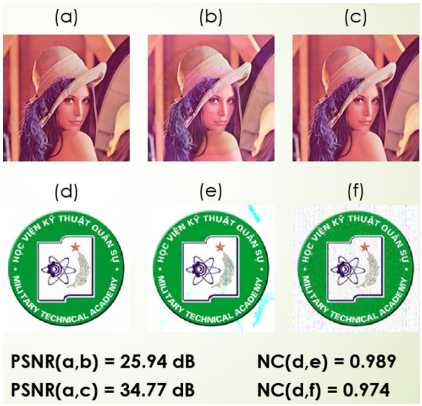

Fig. 4. (a) Lena - original image, (b) DWT-only method based watermarked image, (c) Our method based watermark image, (d) Original watermark logo, (e) DWT-only method based the extracted watermark, (f) Our method based the extracted watermark

Table 1. The values of PSNR and NC for experimental images

Image name	PSNR	NC
Lena	34.7672	0.974729
Pepper	34.7935	0.975822
Couple	34.8068	0.975416
Mandrill	34.8077	0.976204
Parrots	34.9288	0.973707

4.2 Quality of Evaluation

Firstly, we evaluate the quality of the watermarked image after applying our method for embedding the color watermark image shown in the Fig. 2. Our proposed method embeds only S_1 share into the original image instead of embedding all shares in DWT-only method, therefore, the quality of the watermarked image can be improved.

The comparison results are shown in Fig. 4. Since our proposed method only embeds litter amount of watermark comparing with DWT-only method, the quality of watermarked image is better than that of DWT-only method. That shows in the values of our method (34.77 dB) and DWT-only method (25.94 dB). Also, the watermark that is extracted from such DWT-only method and our method show that it is almost the same. NC values are 0.989 and 0.974, respectively.

The values of $PSNR$ and NC are shown in Table 1. Such results show that our proposed method is suitable for the real applications of copyright protection.

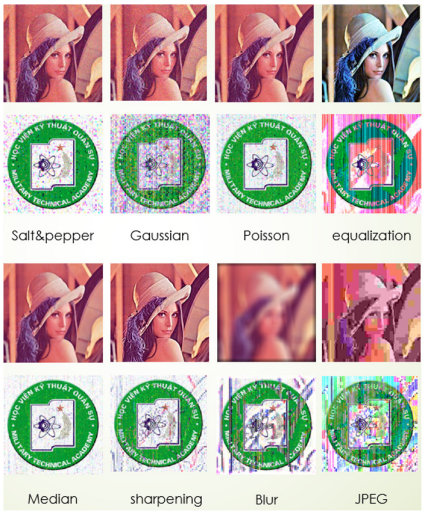

Fig. 5. The extracted watermark image based on corresponding attacks.

Table 2. The NC values computed from attacked Lena image.

Type of attacks	NC
Salt and pepper	0.92044
Gaussian	0.82326
Poisson	0.91805
Equalization	0.70237
Median	0.9567
Sharpening	0.95019
Blur	0.8814
JPEG	0.78889

4.3 Robustness of Comparison

In the following, we evaluate our proposed method against some attacks such as noise addition, low pass filtering, image enhancement, etc. Table 2 shows the NC values of the extracted watermarks under several image processing attacks on Lena image. Figure 5 also shows the extracted watermark image based on corresponding attacks. We can observe that the proposed method is fairly robust against image processing attacks.

In order to prove the efficiency of our method, we compare our experimental results with that of DWT-only method. Table 3 demonstrates that the proposed method is robust against Salt and pepper noise, Gaussian noise, Poisson noise, histogram equalization, Median filtering, Laplacian sharpening, Blur filtering and JPEG compression attacks. Based on these experimental results,

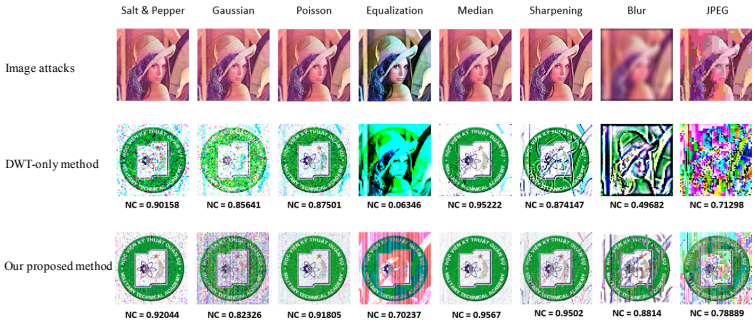

Fig. 6. The comparison of extracted watermarks between the DWT-method and Our method on Lena image.

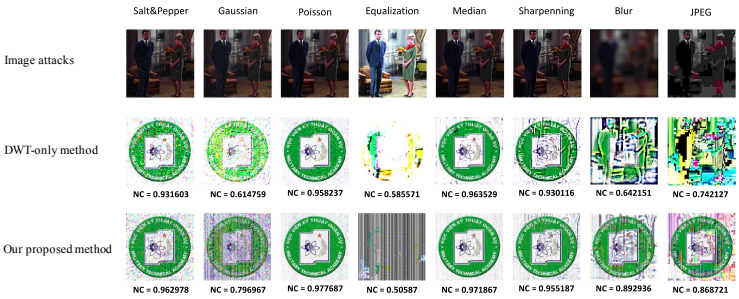

Fig. 7. The comparison of extracted watermarks between the DWT-method and Our method on Couple image.

our proposed method outperforms the reduced DWT-only method for almost testing attacks. This can conclude that the combination of the two technique (DWT-based watermarking and VSS) is more practically helpful than the use of one domain only (DWT) especially if the watermarked images are intended to undergo these types of attacks.

Figure 6, Fig. 7, Fig. 8, Fig. 9, and Fig. 10 describe that the extracted watermarks from our proposed method are more superior than that of DWT-method. The visualization of watermark logos are clear for confirmation the copyright of digital images. The reason is that, in the DWT-method, all bits of color watermark image are embedded into the original images, therefore the quality of the watermarked images is degraded. Also, when the watermarked images are edited undergo some attacks, that makes the extracted watermark images are not so clear.

For robustness confirmation, our values of NC parameters are better than the DWT-method. Therefore, all these experiments show that the proposed method is robust against common image-processing attacks.

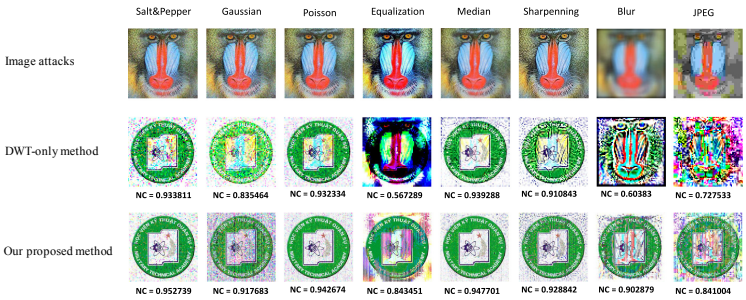

Fig. 8. The comparison of extracted watermarks between the DWT-method and Our method on Mandrill image.

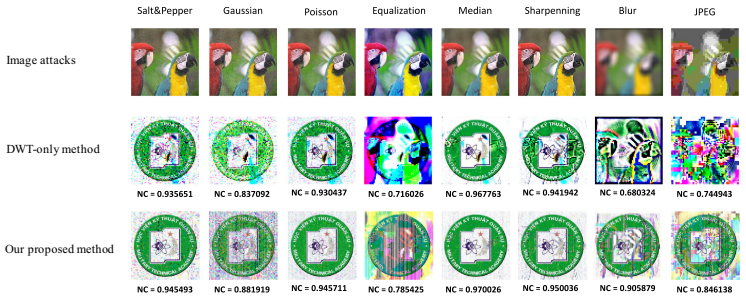

Fig. 9. The comparison of extracted watermarks between the DWT-method and Our method on Parrots image.

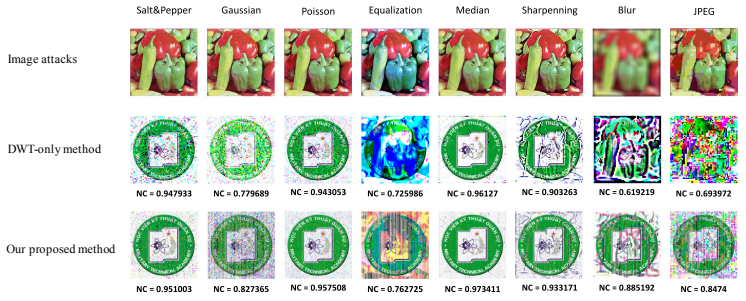

Fig. 10. The comparison of extracted watermarks between the DWT-method and Our method on Pepper image.

Table 3. Comparison of other images.

Attack types	Lena		Pepper		Couple		Mandrill		Parrots	
	DWT-only	Ours	DWT-only	Ours	DWT-only	Ours	DWT-only	Ours	DWT-only	Ours
Salt and pepper	0.90158	**0.92044**	0.94793	**0.95103**	0.9316	**0.99298**	0.93381	**0.95273**	0.93565	**0.94549**
Gaussian noise	0.85641	**0.82326**	0.77968	**0.82737**	0.61476	**0.79696**	0.83546	**0.98768**	0.83709	**0.88191**
Poisson noise	0.87501	**0.91805**	0.94305	**0.95751**	0.95824	**0.97769**	0.93233	**0.94267**	0.93043	**0.94571**
Histogram equalization	0.06346	**0.70237**	0.72598	**0.7627**	0.58557	**0.50587**	0.56728	**0.84345**	0.71602	**0.78542**
Median filter	0.95222	**0.9567**	0.96127	**0.9734**	0.96353	**0.97186**	0.93928	**0.9477**	0.96776	**0.97002**
Sharpening	0.87414	**0.95019**	0.90326	**0.93317**	0.93011	**0.95518**	0.91084	**0.92884**	0.94194	**0.95003**
Blur	0.49682	**0.8814**	0.61922	**0.88519**	0.64215	**0.89293**	0.60383	**0.90287**	0.68032	**0.90587**
JPEG	0.71298	**0.78889**	0.69397	**0.84741**	0.74213	**0.86872**	0.72753	**0.841**	0.74494	**0.84613**

5 Conclusion

In this paper, a robust and simple watermarking scheme based on the combination of DWT domain and VSS is presented. In our solution, the copyright information (copyright logo) is distributed into n shares using $k - out - of - n$ distributed algorithm, also called (k, n) visual secret sharing method. Then, random one share is chosen to embedded into the original images and reduce the degradation of watermarked images.

The experimental results demonstrate that our proposed method provides better robustness against multiple image attacks such as Salt and pepper noise, Gaussian noise, Poisson noise, histogram equalization, Median filtering, Laplacian sharpening, Blur filtering and JPEG compression attacks. Besides, the quality of the watermarked image is satisfactory in terms of imperceptibility for real applications.

In the future works, we plan to extend the watermarking involving visual secret sharing approach to video watermarking domain. It is clear that the embedding and the extracting processes are of low complexity and do not require any specific features of the input image, the extension to video watermarking will be suitable for applying on.

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

References

1. Hsu, C.T., Wu, J.L.: Hidden digital watermarks in images. IEEE Trans. Image Process. **8**(1), 58–68 (1999)
2. Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K.K.: A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU Int. J. Electron. Commun. **68**(3), 244–253 (2014)
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. 1–20 (2016)
4. Singh, A.K., Kumar, B., Singh, S.K., Ghrera, S.P., Mohan, A.: Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Gen. Comput. Syst. (2016)
5. Barni, M., Bartolini, F., Piva, A.: Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans. Image Process. **10**(5), 783–791 (2001)
6. Singh, A.K., Kumar, B., Dave, M., Mohan, A.: Robust and imperceptible dual watermarking for telemedicine applications. Wireless Pers. Commun. **80**(4), 1415–1433 (2015)
7. Singh, A.K., Dave, M., Mohan, A.: Robust and secure multiple watermarking in wavelet domain. J. Med. Imaging Health Inform. **5**(2), 406–414 (2015)
8. Singh, A.K., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools Appl. **75**(14), 8381–8401 (2015). https://doi.org/10.1007/s11042-015-2754-7

9. Urvoy, M., Goudia, D., Autrusseau, F.: Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans. Inf. Forensics Secur. **9**(7), 1108–1119 (2014)
10. 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)
11. Thanh, T.M., Tanaka, K.: The novel and robust watermarking method based on q-logarithm frequency domain. Multimedia Tools Appl. **75**, 11097–11125 (2016)
12. Thanh, T.M., Tanaka, K.: A proposal of novel q-DWT for blind and robust image watermarking. In: Proceeding of IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), Washington D.C., pp. 2066–2070 (2014)
13. Thanh, T.M., Hiep, P.T., Tam, T.M.: A new spatial q-log domain for image watermarking. IJIIP: Int. J. Intell. Inf. Process. **5**(1), 12–20 (2014). ISSN 2093–1964
14. Thanh, T.M., Tanaka, K.: An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. Multimedia Tools Appl. **76**(11), 13455–13471 (2016). https://doi.org/10.1007/s11042-016-3750-2
15. Rani, A., Bhullar, A.K., Dangwal, D., Kumar, S.: A zero-watermarking scheme using discrete wavelet transform. Procedia Comput. Sci. **70**, 603–609 (2015). ISSN 1877–0509. https://doi.org/10.1016/j.procs.2015.10.046
16. Liu, X., Zhao, R., Li, F., Liao, S., Ding, Y., Zou, B.: Novel robust zero-watermarking scheme for digital rights management of 3D videos. Sig. Process.: Image Commun. **54**, 140–151 (2017). ISSN 0923–5965. https://doi.org/10.1016/j.image.2017.03.002
17. Abdelhedi, K., Chaabane, F., Ben Amar, C.: A SVM-based zero-watermarking technique for 3D videos traitor tracing. In: Blanc-Talon, J., Delmas, P., Philips, W., Popescu, D., Scheunders, P. (eds.) ACIVS. LNCS, vol 12002. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-40605-9_32
18. Fu, M.S., Au, O.C.: Joint visual cryptography and watermarking. In: 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763), vol. 2, pp. 975–978 (2004)
19. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053419
20. Shamir, A.: How to share a secret? Commun. ACM **22**(11), 612–613 (1979)
21. Blakley, G.: Safeguarding cryptographic keys. In: Proceedings of AFIPS National Computer Conference (1979)
22. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theory **29**(2), 208–210 (1983)
23. Kandar, S., Dhara, B.C.: k-n secret sharing visual cryptography scheme on color image using random sequence. Int. J. Comput. Appl. **25**(11), 0975–8887 (2011)
24. Kumar, S., Sharma, R.K.: Threshold visual secret sharing based on Boolean operations. Secur. Commun. Netw. (2013). https://doi.org/10.1002/sec.769
25. Elbasi, E., Eskicioglu, A.M.: Naïve Bayes classifier based watermark detection in wavelet transform. In: Gunsel, B., Jain, A.K., Tekalp, A.M., Sankur, B. (eds.) MRCS 2006. LNCS, vol. 4105, pp. 232–240. Springer, Heidelberg (2006). https://doi.org/10.1007/11848035_32
26. Huang, S., Zang, W.: Blind watermarking scheme based on neural network. In: The 7th World Congress on Intelligent Control and Automation, Chongqing, pp. 5985–5989 (2008)

27. Joan, D., Vincent, R.: AES Proposal: Rijndael, National Institute of Standards and Technology (2003). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
28. Hwang, R.J.: A digital image copyright protection scheme based on visual cryptography. Tamkang J. Sci. Eng. **3**(2), 97–106 (2000)
29. Surekha, B., Swamy, G.N., Rao, K.S.: A multiple watermarking technique for images based on visual cryptography. Int. J. Comput. Appl. **1**(1), 78–82 (2010)
30. Bolla, V.R., Gopal, V., Amancha, S.: A two phase copyright protection scheme for digital images using visual cryptography and sampling methods. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 2041–2046 (2016)
31. Wang, M.S., Chen, W.C.: Digital image copyright protection scheme based on visual cryptography and SVD. Opt. Eng. **46**(6) (2007)
32. Surekha, B., Swamy, G.N.: Sensitive digital image watermarking for copyright protection. Int. J. Netw. Secur. **15**(1), 95–103 (2013)
33. Fu, M.S., Au, O.C.: Joint visual cryptography and watermarking. In: IEEE International Conference on Multimedia and Expo (ICME), pp. 27–30 (2004)
34. Tharayil, J.J., Kumar, E.S.K., SusanAlex, N.: Visual cryptography using hybrid halftoning. Procedia Eng. **38**, 2117–2123 (2012)
35. Benoraira, A., Benmahammed, K., Boucenna, N.: Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP J. Adv. Sig. Process. **2015**(1), 1–11 (2015). https://doi.org/10.1186/s13634-015-0239-5