Multimedia Tools and Applications
https://doi.org/10.1007/s11042-022-12079-9

Pseudo Zero-watermarking Technique based on non-blind watermarking and VSS

Ta Minh Thanh[1] · **Giang Ngoc Dan**[1]

Received: 4 January 2021 / Revised: 1 June 2021 / Accepted: 4 January 2022

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. With the advancement in information and network technologies, the unauthorized duplication and manipulation of digital multimedia has 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, many watermarking techniques have been proposed for protecting the author's copyright. The watermarking techniques can be applied on the spatial domain and the frequency domain. In general, the watermarking methods used frequency domain are more robust than that of methods used spatial domain.

✉ Ta Minh Thanh
thanhtm@lqdtu.edu.vn

[1] Le Quy Don Technical University, 236 Hoang Quoc Viet, Ha Noi, Viet Nam

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 [7, 9, 19, 29], DWT-based [2, 16–18], and DFT-based [5, 27]. 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 [25], q-DWT[23], and q-SVD [22]. 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 [24]. 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 [20] is proposed to take a balance of the robustness and the visual quality. In this system, the watermark can only be revealed when enough shared images are obtained. 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 Challenging issues

Based on the analysis above, we summarize the following challenging issues:

(1) *Proposing a new frequency domain for robust watermarking method.*
Almost frequency-based previous methods had tried to provide the robust watermarking methods for applying on the copyright protection solutions. Therefore, the frequency domains, *e.g*. DCT, DWT, DFT, are used to embed the watermark information into the digital contents. However, large amount of watermarking information (especially, color watermark image) that is embedded into the contents will degrade the quality of copyrighted contents. Reducing amount of watermarking information embedded into the contents while remaining the affect for copyright protection solution is required in real applications. Therefore, the first challenge issue is how to propose the frequency domain in order to reduce amount of the watermark information for copyright protection solutions and improve the quality of embedded contents.

(2) *Reducing the dependent of feature from the digital contents.*

In general, the normal zero-watermarking methods [1, 12, 14, 24] extract the robust feature from digital contents, then encode that with the copyright information in order to generate MS and OS. After that, the MS is registered to Copyright Office for confirming the ownership of contents when the dispute occurs. However, since the zero-watermarking methods depend on the feature of digital contents, it may be affected under strong geometric attacks. In order to improve the zero-watermarking that reduce the dependent of feature from the digital contents, we need to find another way to reduce the affects of feature from contents while maintaining the efficiency of copyright protection solutions. Therefore, the second challenge issue is how to reduce the dependent of feature from the digital contents.

(3) *Enhancing the secret of color watermark image*

In general zero-watermarking methods, the watermark information is encoded with the feature extracted from the digital contents. The results of such encoding process are two shares such as master share (MS) and ownership share (OS). Leakage of both of MS and OS can disclose the watermark information. Based on the leakage information, the hackers can generate another copyright information to attack the copyright information. Hence, the last challenge issue is how to provide the method to enhance the secret of color watermark.

1.3 Our contributions

According to above analytic, we summarise our contributions in this paper as follows.

To address the issue (1), 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. By using the combination of frequency domain based embedding approach and VSS, our proposed method can improve the robustness of watermarking method. Also, 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 firstly encoded by AES (Advanced Encryption Standard) [11], 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. That means our method does not employ the feature of original image encrypting with watermark information as conventional zero-watermarking method. 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. Based on such idea, we can address the issue (2).

In order to solve the issue (3), we employ AES encryption to encode the color watermark information. After that, we apply (k, n)-VSS method on the encoded color watermark information to generate n shares using in our system. Only the person who has the AES key and the secret key (k, n) can decode the watermark information and verify the copyright of digital contents. When registering the copyright of the digital contents in Copyright Office, the copyright information is not needed to disclose since the original watermark is encrypted, then are scrambled for generating shares in order to enhance the security. When the dispute happens, only users who provide the correct AES key and the values of k, n to decode the original watermark, can be judged as the owners of digital contents. That makes our proposed method more secure comparing with previous zero-watermarking methods.

1.4 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 Section 5 concludes our paper.

2 Related works

There are various image watermarking methods based on VSS for copyright protection. However, all of them follow the same patterns and steps to secure the cover image. In this section, we present the general scheme of these methods and also the different entities of the system and their roles.

2.1 VSS based zero-watermarking on spatial domain (VZWS)

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 [13, 15]. VC is employed as an extended VSS scheme for digital images. The original problem of VC is the special case of a 2 out of 2 visual secret sharing problem which is the most frequently used. The secret image is divided into two shares that consist of random dots of cover images corresponding location for each pixel of secret image. In order to decode the secret image, the secret information can be easily detected when these shares are stacked together.

Firstly, Hwang [10] had built up an zero-watermarking method based on the concept of visual cryptography. In his method, the watermark information does not have to be embedded directly into the original image. Hwang's method makes it harder to detect or recover from the watermarked image in an illegal way. The watermark information can be retrieved 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 improve the security of the Hwang's method, Surekha et al. [21] 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 and leads to ambiguity in copyright verification. Hence, such algorithms cannot be applied for copyright protection.

In another approach, Bolla et al. [4] proposed a method based on 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 to generate the ownership share (OS) using VC (2.2) with a block of 4 subpixels. The results of this method that the proposed scheme can resist several common attacks.

2.2 VSS based zero-watermarking on frequency domain (VZWF)

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

In the paper of Wang et al. [28], 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 (SV) is selected to generate the MS. The security of this 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, the OS is generated. In the extraction phase, 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. [21] 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 verifies security criteria in order to ensure the reliability of the method. Also, they used PWVC to avoid distortion of the watermark by generating shares that have the same size as the original watermark. In their method, the LL sub-band of DWT domain is randomly selected by using secret key to construct the feature matrix that contains the averages of selected blocks. According to the feature matrix, the MS is generated by the PWVC scheme. In the extraction phase, 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. [24] proposed a new image zero-watermarking scheme based on the encryption of visual map feature (VMF) and permuted visual map feature (PVMF) of the original image with watermark information. They employed the robust feature extracted from the original image by using 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 the proposed method is robust against common processing and geometric attacks with low consuming time.

2.3 Joint visual cryptography and watermarking (JVW)

The concept of Joint Visual-cryptography and watermarking (JVW) algorithm is proposed in paper [8]. In this method, a set of share images is used to protect the content of the

copyright image. Their method also used one share image for hiding in one halftone image. The experimental results from their method showed that is necessary to have both share images in order to reveal the secret images. However, their method constructed the visible watermark when they superimposed both share images. That means the security of their method is not considered enough.

In the paper [6], Cimato et al. proposed an algorithm obtained from the combination with visual cryptography. They proved that the robustness of watermarking method can be improved. Also, multiple trusted authority who participates to the scheme and whose intervention can be requested to arbitrate the ownership of the image if a dispute occurs. However, this method cannot prevent the collaborative attack from multiple trusted authority in order to reveal the original watermark information without permission of original authors. Besides, when a dispute happens, if a trusted authority refuse to provide or destroy the watermark share, the original watermark cannot be decoded to prove the copyrights. Therefore, the solution that can protect the original watermark and prevent the collaborative attack is required such as using the encryption before applying VSS.

In order to increase the security issue, Tharayil et al. [26] proposed method using VC to encrypt the original image into multiple share images. Such multiple share images are distributed among many users. To confirm the copyright information, some share images are needed to collected and are superimposed for visually revealing the copyright image (*e.g* logo). However, their method focused on applying the technique for hybrid halftoned images, therefore, it is not suitable for real applications.

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 of 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 reconstruct the secret image. 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:

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.

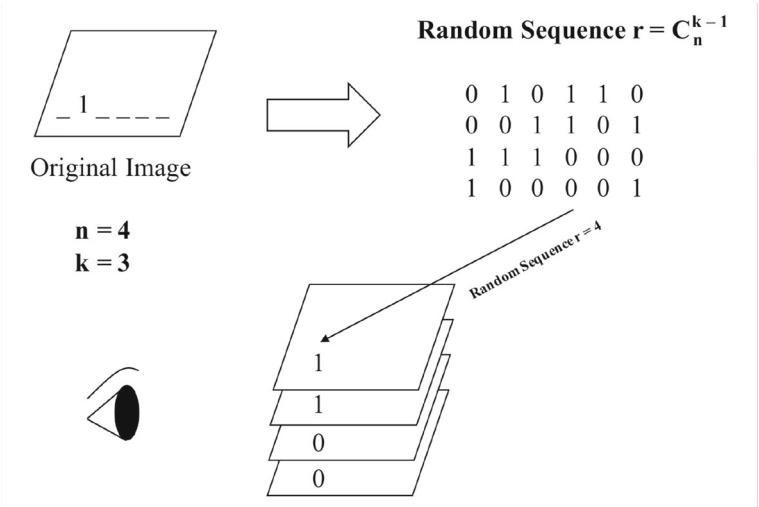

Fig. 1 An illustration of our sharing algorithm

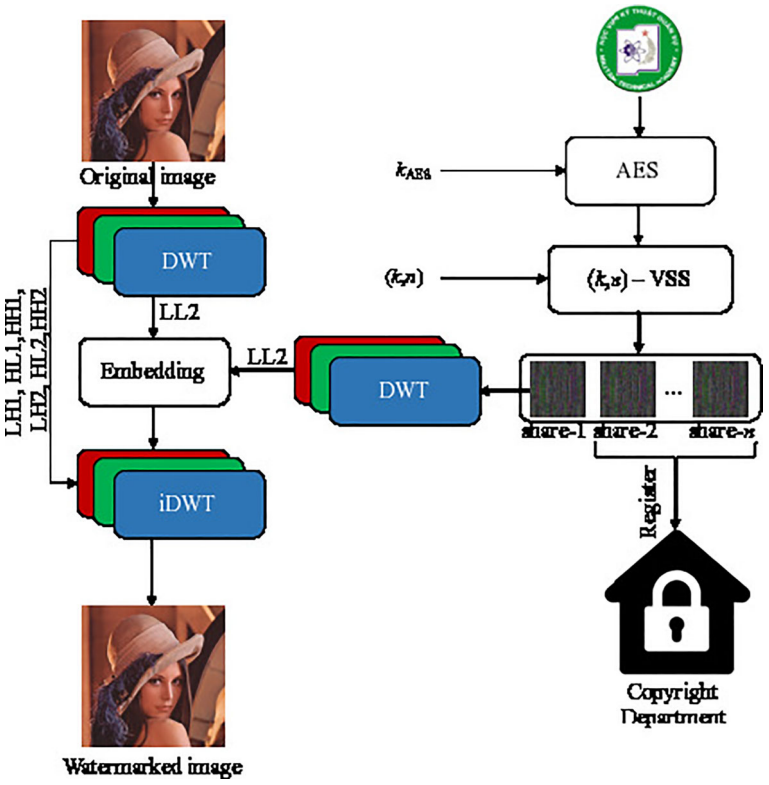

Fig. 2 Our embedding algorithm

In order to protect the original watermark and prevent the collaborative attack from multiple trusted authority, we decide to employ the AES [11] for encoding the watermark before applying our VSS. Only one share is used as the watermark logo and the remain of shares are registered for the trusted authority (TA) (Copyright Department). In our proposed method, we recommend only one trusted authority as a third party to judge the copyrighted users. It will reduce the probability of collaborative attack. Also, to protect the original watermark, the AES encryption is the better solution in term of leakage of the registered watermarks from TA. In our solution, one key is used to distinguish the ownership of the user. In case of a dispute, only users who can provide the key to decrypt the watermark information, will be judged as the copyrighted users. Therefore, when TA requires the decryption key, users have to provide via secure way to prove their copyright.

The detail steps of our method is described as follows:

1. The color watermark image W is firstly encrypted by using AES algorithm 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 Section 3.1.
2. A random share is chosen as a watermark 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). Then, it generates 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.

Suppose the property dispute concerning the suspected image I' happens. The CA should judge the rightful owner of the suspected 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.

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 remain shares ($e.g.$ S_2, S_3, ..., S_n), called OS. A group of k shares are used to decode in (k, n)-VSS scheme, then obtain the encrypted image.
3. Finally, the encrypted image is decrypted by using the 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 equation (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 equation (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.

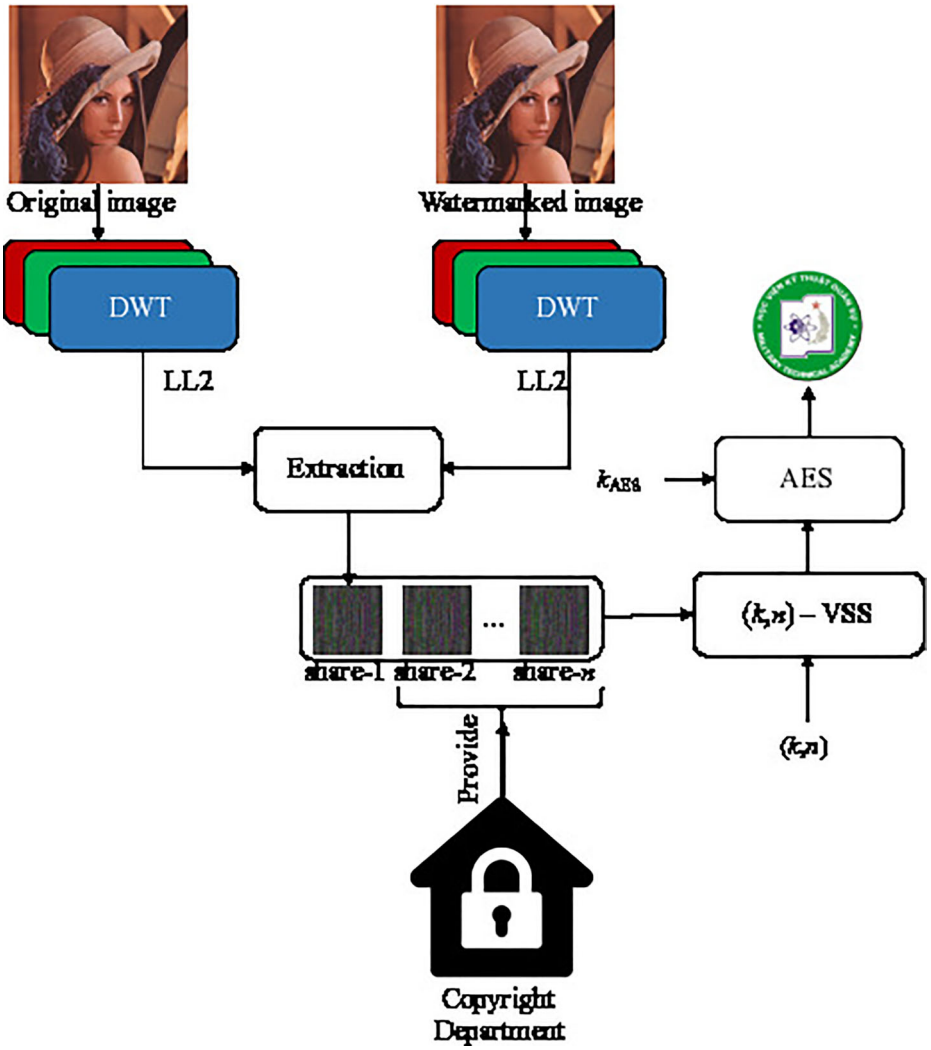

Fig. 3 Our extraction algorithm

4 Experimental results

4.1 Test images and evaluation measures

To assess the performance of the proposed algorithm, we conduct five color images of the well-known SIDBA (Standard Image Data-BAse) database[1]. All test images are with size $W \times H = 256 \times 256$ pixels.

In order to evaluate the quality of watermarked images, we employ $PSNR$ (Peak Signal to Noise Ratio) criterion [24]. The $PSNR$ 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 $MAX(I) = 255$. MSE (Mean Square Error) value 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 judge the robustness, we use the normalized correlation (NC) value between the original watermark W and the extracted watermark W' [24]. The NC value is calculated as follows:

$$NC = \frac{\sum_{i=1}^{L} \sum_{j=1}^{L} W(i, j).W'(i, j)}{\sqrt{\sum_{i=1}^{L} \sum_{j=1}^{L}, W(i, j)^2} \sqrt{\sum_{i=1}^{L} \sum_{j=1}^{L}, W'(i, j)^2}}, \tag{7}$$

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

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

To define the suitable value of watermark strength factor, we used the same method of paper [3]. In the rest of our experiments, we set $\alpha = 0.2$ as the default watermark strength factor value.

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 method only embeds 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 method embeds litter amount of watermark information comparing with DWT-only method, the quality of watermarked image is better than that of DWT-only method. 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.

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

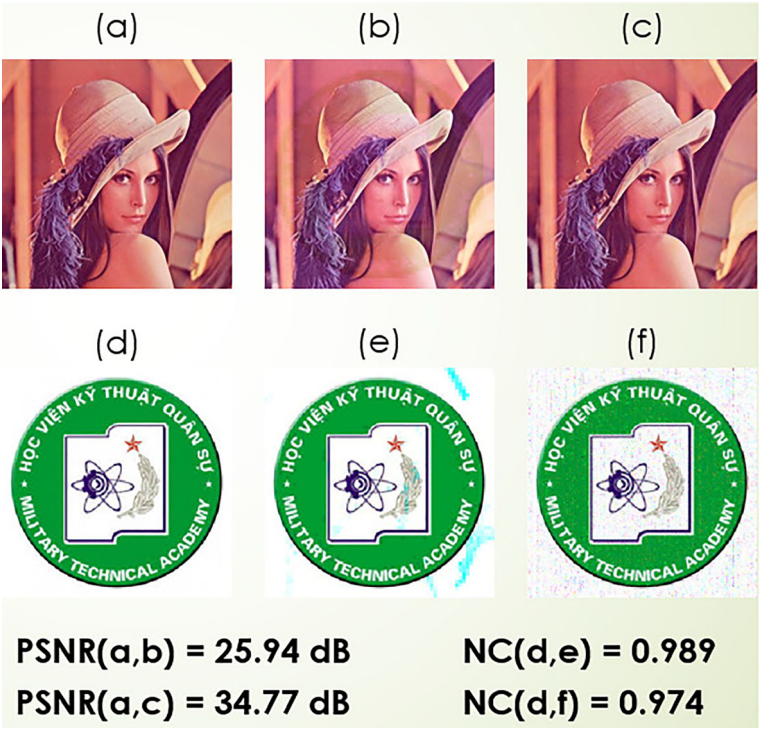

Fig. 4 (a) Lena - original image, (b) DWT-only method based watermarked image, (c) Our method based watermark image, (d) Original watermark logo, (e) DWT-only method based the extracted watermark, (f) Our method based the extracted watermark

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

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

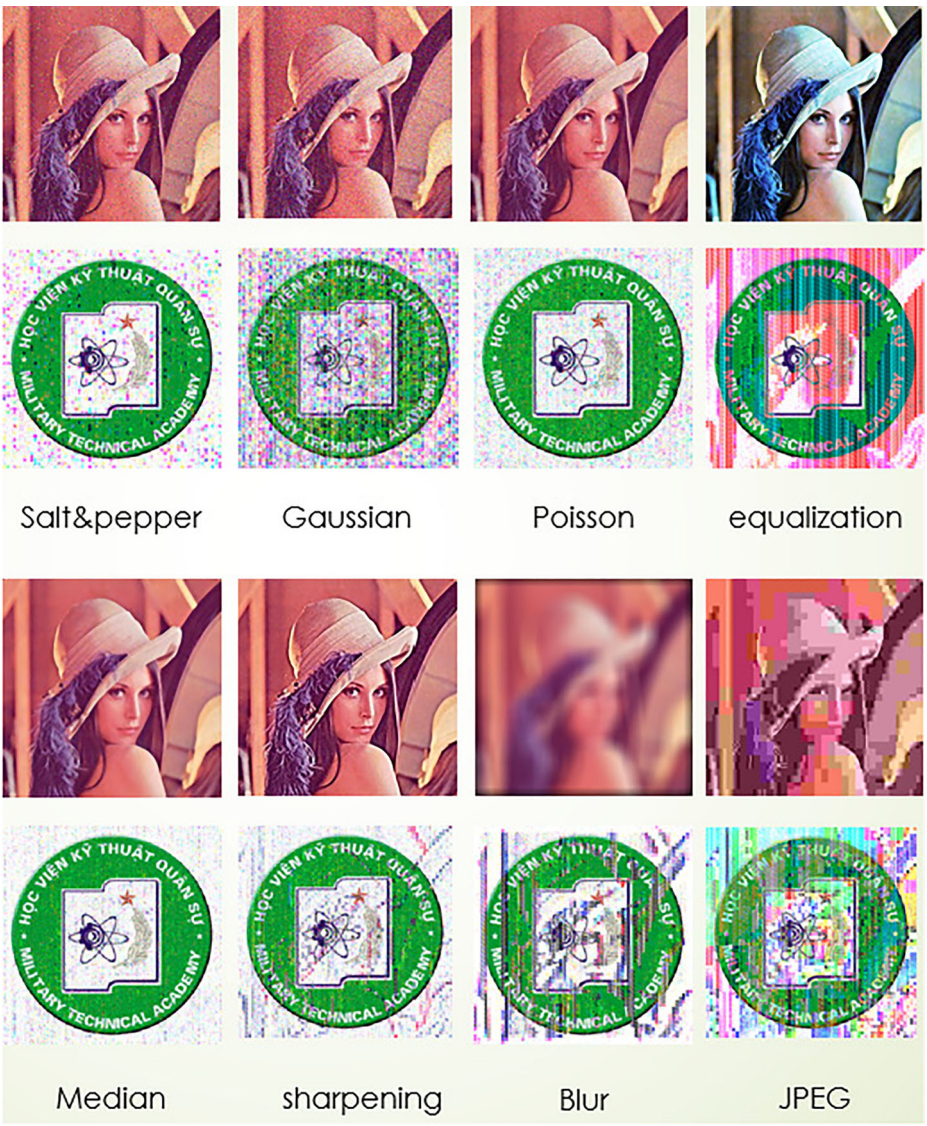

Fig. 5 The extracted watermark image based on corresponding attacks

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

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**

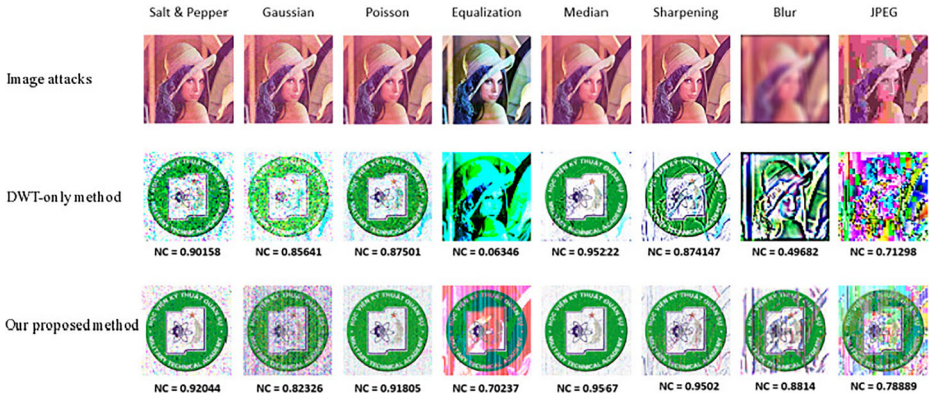

Fig. 6 The comparison of extracted watermarks between the DWT-method and Our method on Lena image

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, 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 (*e.g.* DWT only), especially if the watermarked images are intended to undergo many types of attacks.

Figures 6, 7, 8, 9, and 10 describe that the extracted watermarks from our proposed method are more superior than that of DWT-method. The visualization of watermark images 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 NC values are better than the NC values of DWT-method. Therefore, all experiments show that the proposed method is robust against common image-processing attacks.

In order to make more clearly the efficiency of our method, we compare the methodology with the paper [6]. The comparison is shown in Table 4. It is clear that our method is more

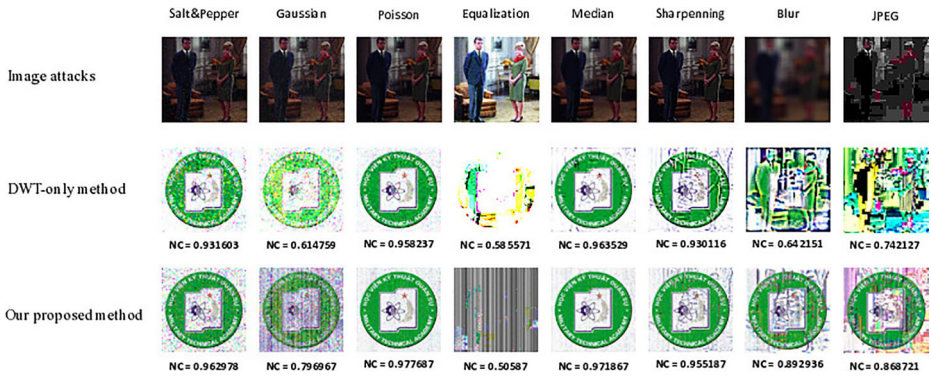

Fig. 7 The comparison of extracted watermarks between the DWT-method and Our method on Couple image

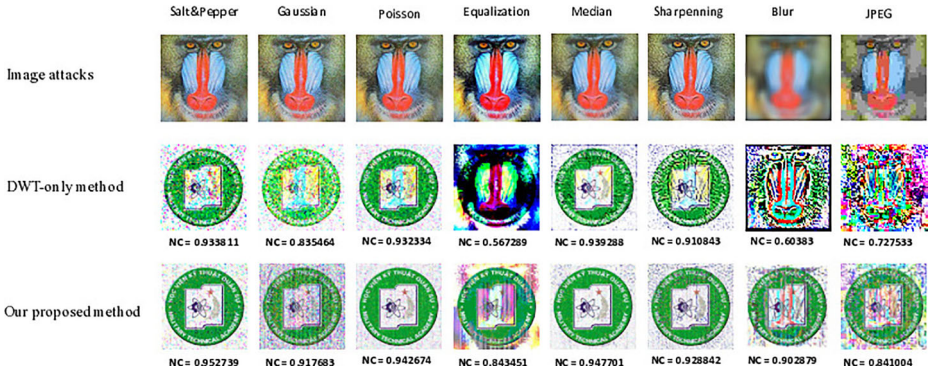

Fig. 8 The comparison of extracted watermarks between the DWT-method and Our method on Mandrill image

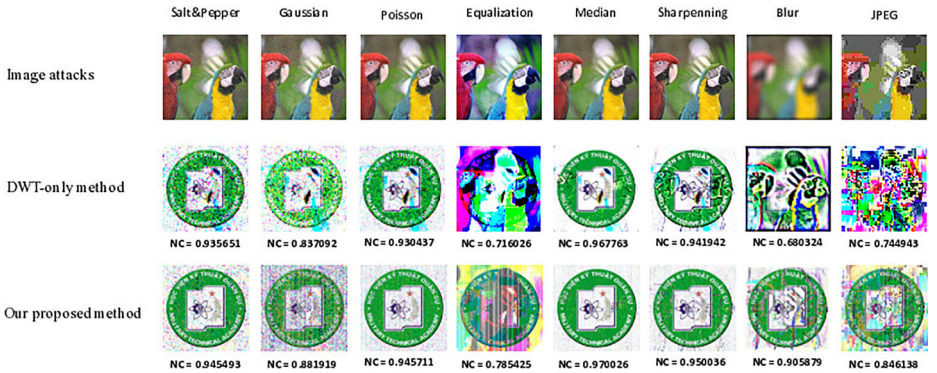

Fig. 9 The comparison of extracted watermarks between the DWT-method and Our method on Parrots image

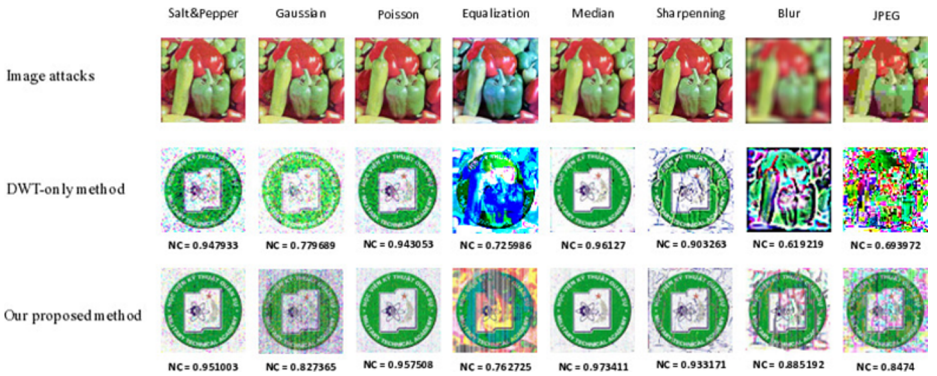

Fig. 10 The comparison of extracted watermarks between the DWT-method and Our method on Pepper image

Table 4 Comparison with method of paper [6]

Comparison items	Our proposed method	Method of paper [6]
Combination with VSS	$(k, n)-$VSS, Flexible	$(2, 2)-$VSS, Fixed
Trusted authority (TA)	Only one TA	Multiple TA
Watermark image	Color watermark	Grayscale watermark
Secret enhancement	AES with VSS	Only VSS
Key management system	Users side management	TA side management

flexible than the method in [6]. We recommend only one TA for reducing the collaborative attack. Therefore, we employ the AES algorithm for protecting the watermark information, then enhance the secret of copyright protection solution. We believe that such model is efficiency for digital rights management system.

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, one random share is chosen to embedded into the original images. As a result, our method can 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. Abdelhedi K, Chaabane F, Ben Amar C (2020) A SVM-Based Zero-Watermarking Technique for 3D Videos Traitor Tracing, Advanced Concepts for Intelligent Vision Systems (ACIVS 2020), Lecture Notes in Computer Science, vol 12002. Springer, Berlin. https://doi.org/10.1007/978-3-030-40605-9_32
2. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans Image Process 10(5):783–791
3. Benoraira A, Benmahammed K, Boucenna N (2015) Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP Journal on Advances in Signal Processing, vol 55
4. Bolla VR, Gopal V, Amancha S (2016) A Two Phase Copyright Protection Scheme for Digital Images using Visual Cryptography and Sampling Meth161 ods. In: International Conference on Electrical Electronics, and Optimization Techniques (ICEEOT), pp 2041–2046

5. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2014) Robust digital image watermarking using interest points and DFT domain. In: 35Th IEEE international conference on telecommunications and signal processing (TSP), pp 715–719
6. Cimato S, Yang JCN, Wu C (2014) Visual cryptography based watermarking, transactions on data hiding and multimedia security IX, 91–109
7. Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU Int J Electron Commun 68(3):244–253
8. Fu MS, Au OC (2004) Joint visual cryptography and watermarking. IEEE International Conference on Multimedia and Expo (ICME), 27–30
9. Hsu CT, Wu JL (1999) Hidden digital watermarks in images. IEEE Trans Image Process 8(1):58–68
10. Hwang RJ (2000) A digital image copyright protection scheme based on visual cryptography. Tamkang J Sci Eng 3(2):97–106
11. Joan D, Vincent R (2003) AES Proposal: Rijndael, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
12. Liu X, Zhao R, Li F, Liao S, Ding Y, Zou B (2017) Novel robust zero-watermarking scheme for digital rights management of 3D videos. Signal Processing Image Communication 54:140–151. https://doi.org/10.1016/j.image.2017.03.002. ISSN 0923–5965
13. Naor M, Shamir A (1995) Visual Cryptography. In: De Santis A (ed) Advances in Cryptology (EUROCRYPTO 94), (Lecture Notes in Computer Science), vol 950. Springer, Berlin, pp 1–12
14. Rani A, Bhullar AK, Dangwal D, Kumar S (2015) A Zero-Watermarking Scheme using Discrete Wavelet Transform. Procedia Computer Science 70:603–609. https://doi.org/10.1016/j.procs.2015.10.046. ISSN 1877–0509
15. Shamir A (1979) How to share a secret? Comm ACM 22(11):612–613
16. Singh AK, Dave M, Mohan A (2015) Robust and secure multiple watermarking in wavelet domain. J Med Imaging Health Inform 5(2):406–414
17. Singh AK, Dave M, Mohan A (2015) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 121
18. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
19. Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A (2016) Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network. Future Generation Computer Systems
20. Sun M, Fu OCA (2004) Joint visual cryptography and watermarking, 2004. IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763) 2:975–978
21. Surekha B, Swamy GN (2013) Sensitive digital image watermarking for copyright protection. Int J Netw Secur 15(1):95–103
22. Thanh TM, Hiep PT, Tam TM, New Spatial A (2014) Q-log Domain for Image Watermarking, IJIIP. International Journal of Intelligent Information Processing 5(1):12–20. ISSN 2093–1964
23. Thanh TM, Tanaka K (2014) 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 DC, pp 2066–2070
24. Thanh TM, Tanaka K (2016) An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. In: International Journal of Multimedia Tools and Applications (MTAP). ISSN 1573–7721
25. Thanh TM, Tanaka K (2016) The novel and robust watermarking method based on q-logarithm frequency domain. Multimed Tools Appl 75:11097–11125
26. Tharayil JJ, Kumar ESK, SusanAlex N (2012) Visual cryptography using hybrid halftoning. Procedia Eng 38:2117–2123
27. Urvoy M, Goudia D, Autrusseau F (2014) Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans Inform Forens Secur 9(7):1108–1119
28. Wang MS, Chen WC (2007) Digital image copyright protection scheme based on visual cryptography and SVD. Opt Eng 6:46
29. Zear A, Singh AK, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl, 1–20