ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A ROBUST WATERMARKING SCHEME BASED ON DCT, IWT and SVD WITH OPTIMAL BLOCK

MOHAMED RADOUANE[1], NADIA IDRISSI ZOUGGARI[2], AMINE AMRAOUI[3], MOUNIR AMRAOUI[4]

[1]Professor, SPM Team, Department of Web and Mobile Engineering, ENSIAS, Mohammed V University in RABAT, Morocco

[2]Researcher. Faculty of Science, Mohammed V University in RABAT, Morocco

[3]Phd Student. Faculty of Science, Ibn Tofail University, Morocco

[4]Professor. High School of Technology, Mohammed V University in RABAT, Morocco

E-mail: [1]mohamed.radouane@ensias.um5.ac.ma

ABSTRACT

Signal processing's impact on development of digital media technologies have become a hot topic. The increased of computer network and the growth of the Internet have facilitated the production and distribution of unauthorized copies of multimedia information (text, image, sound, and video). To ensure multimedia security, researchers are focusing on digital image watermarking. With this new concept, the watermark is not just hiding in an image, but it's marked indelibly. In this paper a robust method of digital images watermarking based on combination of DCT, IWT and SVD is proposed. At first, Visual cryptography is used to encrypt the watermark image. Then DCT is applied to it and to the host image. IWT and SVD are applied on DCT coefficients of both watermark and host images. After that, the watermarking process is done by embedding singular values of watermark image to the singular values of host image. Moreover, the obtained watermarked images are subjected to different attacks to improve the robustness of the proposed scheme. Finally, the extraction process is based on watermarked image and the reverse method of embedding process to reconstruct the original watermark. The performance is evaluated under various attacks and experimental results show that our algorithm provides a high level of robustness and imperceptibility than the state-of-the-art methods.

Keywords: *DCT, IWT, SVD, Entropy, Watermarking.*

1. INTRODUCTION

Recently, digital image copyright protection is required for Cloud computing, Internet of Things and multimedia transmission. Duplicating, modifying, reproducing and distributing digital images has become increasingly easy legally or illegally. For this reason different methods to ensure this protection are implemented [1] [2]. Firstly, we have steganography that allows hiding information [3] [4], then cryptography to secure and encrypt communication [5]. This technique protects the image being transmitted. But once the image is decrypted, it has no protection. The weakness lies in the lack of robustness. Indeed, it is easy to remove the inserted message by the systematic change of the original image. Therefore, the need for more effective methods to protect the copyright is essential [6] [7].Hence the recent emergence of the concept of digital watermarking [8] [9].

Today, digital image watermarking has become an effective multimedia security scheme from illegitimate use over the Internet. Digital image watermarking is the processing of combined information into a digital signal, it is a set of techniques and methods to insert a secret message in an image to identify and characterize the intellectual property [10] [12]. This insertion should not disturb the original image (Figure 1). Owner or distributor must know the inserted message, and it must meet four basic requirements: imperceptibility, robustness, capacity and security.

Robustness is measured when the watermarked image is attacked. Therefore, the embedded watermark can resist several multimedia attacks.

Imperceptibility is obtained when we have an invisibility perception between original and watermarked image, then the watermark shouldn't degrade the quality of the original image.

Capacity is the acceptable growth of embedded information in the watermarked image.

Security is one of the main requirements, which is based on the power and objectives of the person who wants to modify, copy or delete the watermark.

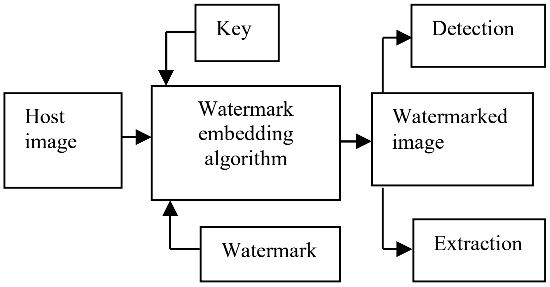


Figure. 1 Standard Watermarking Scheme

Digital watermarking methods are classified into spatial domain, frequency domain and multi-resolution domain. Each method has advantages and disadvantages depending on the requirements of the application to be used.

Image processing in the spatial domain [13] [14] allows direct transformation of pixel luminance. The watermarking methods used in this domain are computationally inexpensive since they do not require a prior transformation step, but they are less imperceptible and robust against various attacks. Due to the above mentioned limitations of spatial domain, different researchers are now oriented to frequency and multi-resolution domain. In the frequency domain [15] [16], the signal is analyzed in relation to the frequency. The processing is done on the transformed image and the watermark image is embedded in the original image by modifying these coefficients. Various transformations such as DCT, DWT and SVD can be used. Finally, to reorganize the original image an inverse transformation is applied.

After that, researchers have switched to a more powerful multi-resolution domain to analyze the fine details of the image. Multi-resolution domain [17] [18] is an important area of watermarking. It consists in applying successive subsampling on the original image to allow the isolation of the low frequency components constituting an insertion space less sensitive than the image itself.

These transformation methods guarantee a best increased security, better imperceptibility and robustness against various attacks. But a single spatial or transformation domain method cannot simultaneously meet all the basic design requirements. To solve this problem, the concept of hybrid methods in the transformation domain has been developed.

Hybrid domain methods [19] [20] are considered as combinations of the different presented domains and are designed to provide greater robustness and better imperceptibility with high security. Also, hybrid transform domain methods combine more than one transformation for improving the performance of the watermarking system. For example, DCT converts the image from the spatial domain to the frequency domain to get the cosine coefficients. Those coefficients are classified into low-frequency, middle-frequency, and high-frequency coefficients. DCT ensures better imperceptibility and is robust against noise, filtering, JPEG compression, and geometric attacks. Besides, IWT ensures high imperceptibility and robustness against JPEG compression, salt-and-pepper noise (SPN), Gaussian noise (GN), and statistical attacks. On the other hand, SVD ensures robustness against noise, sharpening, cropping, filtering, and JPEG compression attacks.

Our contributions in this paper consist to present a hybrid robust method of digital image watermarking based on combination of DCT, IWT and SVD using optimal block. This method ensures improved imperceptibility, robustness, large capacity and security simultaneously. The watermark image is encrypted with visual cryptography to ensuring security. Then, an invisible watermark is embedded to the host image. Finally, a blind watermarking system that does not require the host image is designed to extract the watermark from the watermarked image. Generally, this contribution can also be important to protect images and claim ownership. Without watermarks, digital images may be vulnerable to theft or unauthorized use.

The remaining of the paper is organized as follows. After the introduction of the problem, Section 2 illustrates the related work in the literature. Section 3 presents theoretical background. In section 4, we describe the proposed approach for watermarking scheme in detail, and we clarify experiment results as well as some discussions in section 5. Section6 presents threats to the validity of the study. Finally, conclusion is given with future work.

2. RELATED WORK

Protection of high-quality images transmission over the Internet requests new approaches like hybrid image watermarking to ensure the basic requirement simultaneously.

In [21], a multipurpose image-watermarking algorithm is proposed to provide tamper localization, self-recovery and ownership verification of the host image. This method is based on wavelet domain using DWT (Discrete Wavelet Transform) and singular values decomposition. The robust insertion is also optimized with the help of ABC (Artificial Bee colony) in such a way that maximum robustness can be assured corresponding to user specific threshold of imperceptibility.

In [22], E.Najafi et al presents a robust image watermarking scheme based on singular value decomposition (SVD) and sharp frequency localized contourlet transform (SFLCT). The robustness of the scheme is improved against all considered geometrical and image processing attacks.

In [23], S.Madhavan et al presents a method of digital image watermarking used in copyright protection. In this method, the grey image is divided into four sub-bands using DWT, and the desired sub-bands are selected. The watermark bits are embedded in LH, HL sub-bands. The cuckoo search algorithm is used to recognize optimal positions in the discrete wavelet transform (DWT) domain for watermark insertion in the binary image. The results display the importance of using this algorithm for the watermarking techniques for copyright protection. It is established in the present scheme a superior improvement on imperceptibility.

In [24], M.Radouane et al proposed a robust method for digital images watermarking. This method is achieved by searching the optimal block that can be used to insert the watermark in original image using SVD and DWT combined with DCT (Discrete Cosine Transform). The experimental results show that this imperceptible method combines the advantage of three transformations to ensure robustness against most attacks. In this work, intellectual property of images is protected by the approach proposed.

In [25] digital watermarking based on joint DWT-DCT and OMP reconstruction is presented by (Zhang et al). In this paper various levels of DWT are applied on the host image, and then DCT is merged with DWT. Spread transform quantization index modulation algorithm is introduced to implement the watermark embedding. On the other hand, orthogonal matching pursuit compression reconstruction algorithm is presented for the watermarking algorithm to optimize the watermark extraction. This method is not robust again the most attacks and security is not considered for the watermark.

In [26] Zheng et al present a hybrid image watermarking method based on DCT, DWT and SVD for resisting rotational attacks. In this method the security is not considered because the watermark is not encrypted with any encryption technique. For ensuring security, different methods are proposed.

In [27] a secure and robust color image watermarking is developed to achieve high color watermarking imperceptibility while maintaining a high resistance to attacks. The proposed scheme employs the interconnection between the sub-bands of the primary color components in the wavelet packet domain. To increase watermark security, a scribbling watermark is used.

In [28] a hybrid combination of the wavelet transforms has been discussed for single and multiple image watermarking. The transforms combined in this paper, are non-subsampled contourlet transform (NSCT), discrete cosine transform (DCT) and multi-resolution singular value decomposition (MSVD). This method embeds the same watermark bits to the two different positions of the host image for ensuring security. This blind image watermarking method provides better imperceptibility and improved robustness against most attacks. Also, the method has less computational complexity in terms of time. But, the method does not analyze the watermark embedding capacity. Hence, the capacity is improved by Prabha et al [29]. In this paper a new blind color image watermarking based on the Walsh Hadamard Transform (WHT) is proposed. At first, the proposed method subdivides the image into non-overlapping blocks, which are then transformed using WHT. Then, the color 4□4 image watermark is embedded in the third and fourth-row WHT coefficients. The method has strong robustness against various image attacks.

The analysis of the methods proposed in this section allows us to conclude that these approaches do not ensure simultaneously the design requirement of the watermarking system such as imperceptibility, large capacity, robustness and security.

The main finding of 9 selected papers is:

- PSNR and NC are the most frequently metrics used to evaluate the performance of the watermarking technique.
- Most of the studies combined more than two techniques of watermarking.
- Most of the studies use only two or three design requirement.

- Geometric attacks are the most types of attacks used in the evaluation of performance.

Due to the limitations presented in these work, we have designed a hybrid watermarking scheme that respect the entire requirement for a typical watermarking system. The proposed scheme is based on combination of DCT, IWT and SVD technique using optimal block selection to embed the watermark. IWT is used in this approach because it exploits the characteristic of DWT for increasing the imperceptibility and it's much faster. DCT and SVD are applied for increasing robustness against most attacks.

3. TABLES AND FIGURES

This sub-section present the different transformation methods used in this paper and the visual cryptography used to encrypt the watermark.

3.1 DCT (Discrete Cosine Transform):

DCT [30] allows the separation of high, low and medium frequencies. The low frequencies are at the top left of the matrix, and the high frequencies at the bottom right. This transform is applied to a square matrix. The result is represented in a matrix of the same dimension.

DCT is an orthogonal matrix transformation; it is accompanied by a method of inversion to return to the spatial domain. Thus, after making changes in the frequency domain, eliminate variations in the image almost invisible to the human eye, we return to a representation in the form of pixels.

The Discrete Cosine Transform of an image OI of dimension MxN is performed using the following formula:

$$\mathrm{DCT}(\mathrm{i},\mathrm{j}) = \frac{1}{\sqrt{2\mathrm{N}}}\mathrm{B}(\mathrm{i})\mathrm{B}(\mathrm{j})\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\mathrm{M}(\mathrm{x},\mathrm{y}).\cos\left[\frac{(2x+1)}{2N}i\pi\right]\cos\left[\frac{(2y+1)}{2N}j\pi\right]$$

Where M(x,y) is the original image

$$\mathrm{B}(\mathrm{u}) = \begin{cases}\frac{1}{\sqrt{2}}\ if\ (u=0)\\ 1\ if\ (u>0)\end{cases}$$

The inverse DCT is given by

$$\mathrm{M}(\mathrm{x},\mathrm{y}) = \frac{1}{\sqrt{2\mathrm{N}}}\mathrm{B}(\mathrm{i})\mathrm{B}(\mathrm{j})\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\mathrm{DCT}(\mathrm{i},\mathrm{j}).\cos\left[\frac{(2x+1)}{2N}i\pi\right]\cos\left[\frac{(2y+1)}{2N}j\pi\right]$$

Where

$$\mathrm{B}(\mathrm{u}) = \begin{cases}\frac{1}{\sqrt{2}}\ if\ (u=0)\\ 1\ if\ (u>0)\end{cases}$$

3.2 DCT (Discrete Cosine Transform):

SVD [31] [32] is a mathematical technique that provides a safe way to extract algebraic features from an image. The main properties of the SV matrix of an image can be exploited in the field of digital watermarking. This matrix has a good stability; when a small perturbation occurs in an image, the variation of its SV can be neglected. By using this property of the SV matrix of an image, the watermark can be inserted in this matrix without a big variation of the watermarked image.

The singular values represent the energy of the image, i.e. the SVD arranges the maximum energy of the image into a minimum of singular values.

The singular value decomposition of a matrix I of size m x n is written as follows:

$$\mathrm{I} = \mathrm{U} * \mathrm{S} * V^T$$

Where V^T is the transpose matrix of V.

3.3 IWT (Integer Wavelet Transform):

Integer wavelet transform (IWT) [33] [34] maps the original image into integer coefficients. It can be constructed by using lifting schemes. IWT is usually used in watermarking process because it has different advantages in the data decomposition (reversible, faster and has no rounding errors). IWT consists of three steps: split, prediction and update (Figure 2).

Split: The original signal is decomposed into two samples sets even and odd sets S_0 and S_e.

Prediction: The odd samples are predicted from the even. S_0 is predicted from the S_e.

Update: new even samples S_e is generated based on an updater.

The inverse lifting steps are finished by reversing lifting steps. Finally, the split is substituted for the merge.

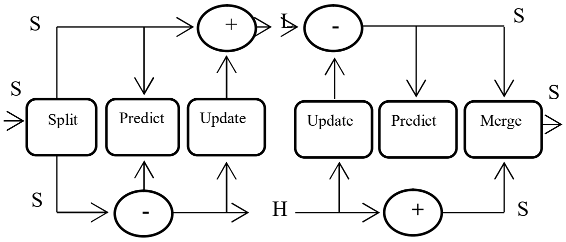


Figure2: Lifting And Inverse Lifting

3.4 Visual Cryptography

In this paper, the watermark is generated with the help of (2, 2) visual cryptography technique to encrypt the watermark that will be used in the watermarking process. For this two shares of watermark W_a and W_b are generated.

The process of VC consists of two sub-pixels S_{b1} and S_{b2} derived from black and white pixel obtained from the watermark image W(x,y). Hence, an attacker looking at single share cannot know whether the secret pixel is black or white because both the shares are required to obtain the final watermark image. If original secret pixel is black, two black subpixels will appear and if original secret pixel is white, one white subpixel and one black pixel will appear. An example of the (2, 2) VC scheme is shown in Figure 3.

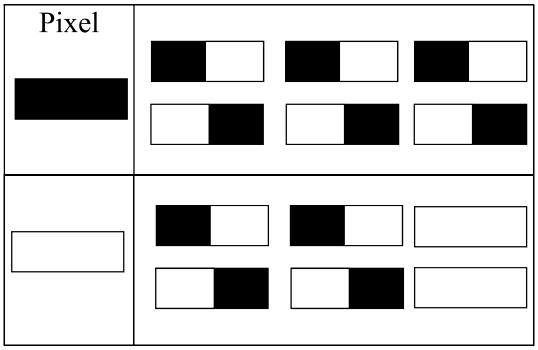


Figure 3. Concept Of (2,2) VC.

4. EQUATIONS

In this section we present the proposed watermarking scheme. The watermarking embedding algorithm and extraction algorithm are described in section 4.1 and 4.2 respectively.

4.1 Watermarking embedding algorithm:

Firstly, the watermark image is preprocessed that consists of securing it by visual cryptography technique, then applying DCT, IWT and SVD methods to the scrambled watermark image. One of the share watermarks is retained with the user to recover the final watermark image. Then, DCT is applied to the encrypted watermark to get a new image 'wdc'. The 'wdc' image is decomposed by 2-level IWT four sub-bands: LL_{wdc}, LH_{wdc}, HL_{wdc}, HH_{wdc}, where LH represents approximate details. LH emphasizes vertical details. HL gives the horizontal details and HH provides the diagonal details. The 2-level IWT consists of the following equations:

$$LL_{wdc}, LH_{wdc}, HL_{wdc}, HH_{wdc} = IWT(wdc)$$
$$LL_{2wdc}, LH_{2wdc}, HL_{2wdc}, HH_{2wdc} = IWT(LL_{wdc})$$

SVD is applied on HH_{2wdc} to get three matrices:

$$[U_w, S_w, V_w] = SVD(HH_{wdc})$$

Where, S_w is the singular values of SVD.

On the other hand, DCT is applied on the host image to get I_c image. Then, 2-level IWT is applied on I_c to generate four sub-bands LL_{Ic},LH_{Ic},HL_{Ic},HH_{Ic}.

$$LL_{Ic}, LH_{Ic}, HL_{Ic}, HH_{Ic} = IWT(I_c)$$
$$LL_{2Ic}, LH_{2Ic}, HL_{2Ic}, HH_{2Ic} = IWT(HH_{Ic})$$

SVD is applied on HH_{2Ic} to get three matrices:

$$[U_i, S_i, V_i] = SVD(HH_{Ic})$$

Where, S_i is the singular values of SVD.

S_i values are devised on different blocks, and then the entropy value is calculated for each block. The embedding process is done automatically on blocks that have a maximum entropy value, which is the strong point for our method. The watermark can be inserted in SV matrix without a big variation of the watermarked image and the embedding in this area has a good impact on the watermarking algorithm.

The watermark embedding function is based on singular values of the host image and the watermark image. Then, a watermark strength alpha is required to ensuring better imperceptibility. The final watermark block S_{emb} is obtained by:

$$S_{emb} = S_i + alpha * S_w$$

Finally, the inverse used methods ISVD, IIWT, IDCT are applied to obtain the watermarked image.

The proposed watermarking method is presented in Figure 4. Our method is based on blind watermarking process and an invisible watermark image which is extracted from the watermarked image without using the original image.

The whole process of watermark embedding is explained bellow:

Step1: The watermark is encrypted with visual cryptography technique which explained in section 3.4.

Step2: Apply DCT on the encrypted watermark to obtain a new image wdc.

Step3: Apply 2-level IWT on wdc image to obtain four coefficients.

$$LL_{wdc}, LH_{wdc}, HL_{wdc}, HH_{wdc} - IWT(wdc)$$

$$LL_{2wdc}, LH_{2wdc}, HL_{2wdc}, HH_{2wdc} = IWT(LL_{wdc})$$

Step4: Apply SVD on HH_{2wdc} sub-band

$$[U_w, S_w, V_w] = SVD(HH_{wdc})$$

Step5: Apply DCT to the original image to get I_c image

Step6: Apply 2-level IWT to I_c image

$$LL_{1c}, LH_{1c}, HL_{1c}, HH_{1c} = IWT(I_c)$$

$$LL_{2Ic}, LH_{2Ic}, HL_{2Ic}, HH_{2Ic} = IWT(HH_{Ic})$$

Step7: Apply SVD to HH_{2Ic} sub-band.

$$[U_i, S_i, V_i] = SVD(HH_{Ic})$$

Step8: Apply embedding function

$$S_{emb} = S_i + alpha * S_w$$

Step9: to back to the spatial domain, we should inverse our earlier procedure.
Apply SVD on S_{emb}:

$$[US_{emb}, SS_{emb}, VS_{emb}] = SVD(S_{emb})$$

Step10: Apply ISVD on S_{emb}

$$W_m - U_m * SS_{emb} * V_m$$

Step11: Apply IIWT on W_m

$$W_{1m} = IIWT(LL_{2Ic}, LH_{2Ic}, HL_{2Ic}, HH_{2Ic})$$

$$W_{2m} - IIWT(W_{1m}, LH_{1Ic}, HL_{1Ic}, HH_{1Ic})$$

Step12: Apply IDCT on W_{2m} to get the watermarked image WI.

$$WI = IDCT(W_{2m})$$

4.2 watermarking extraction algorithm

Step1: Apply DCT on watermarked image to obtain DCWI image.
Step2: Apply 2-level IWT on DCWI

$$LL_{DCWI}, LH_{DCWI}, HL_{DCWI}, HH_{DCWI} = IWT(DCWI)$$
$$LL_{2DCWI}, LH_{2DCWI}, HL_{2DCWI}, HH_{2DCWI} = IWT(LL_{DCWI})$$

Step 3: Apply SVD to the , HH_{2DCWI} sub-band.

$$[U_{we}, S_{we}, V_{we}] - SVD(HH_{2DCWI})$$

Step4: Extract S_w

$$S_w = \frac{S_{emb} - S_i}{aplpha}$$

Ste5: Apply inverse SVD

$$W_e = U_w * S_w * V_w'$$

Step6: Apply inverse IWT

$$W_{e1} = IIWT(LL_{2w}, LH_{2w}, HL_{2w}, W_e)$$

$$W_{e2} = IIWT(W_{e1}, LH_w, HL_w, HH_w)$$

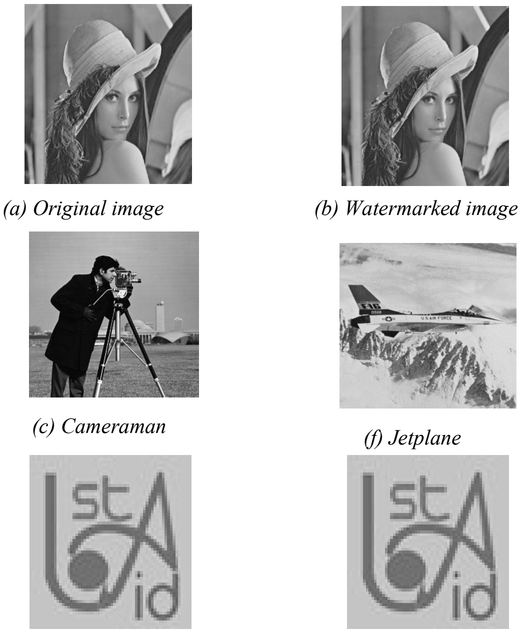
Step7: Apply inverse DCT

$$W_F = IDCT(W_{e2})$$

Step8: Decrypt watermark.

5. EXPERIMENTAL RESULTS

In this section, the performance about imperceptibility, robustness and security is evaluated under different types of attacks: Salt and pepper, Gaussian noise, median filtering, resizing, contrast adjustment, JPEG compression, cropping, rotation, and Histogram equalization, etc. Then, the proposed method is compared with existing method in the literature. The original image considered for experimentation is Lena cameraman and jetplane images of size 512 x 512. The watermark image is a logo of size 32 x 32 (Figure 7).



(a) Original image *(b) Watermarked image*

(c) Cameraman *(f) Jetplane*

(e) Watermark image *(d) Extracted watermark*

Figure 4: Test Images

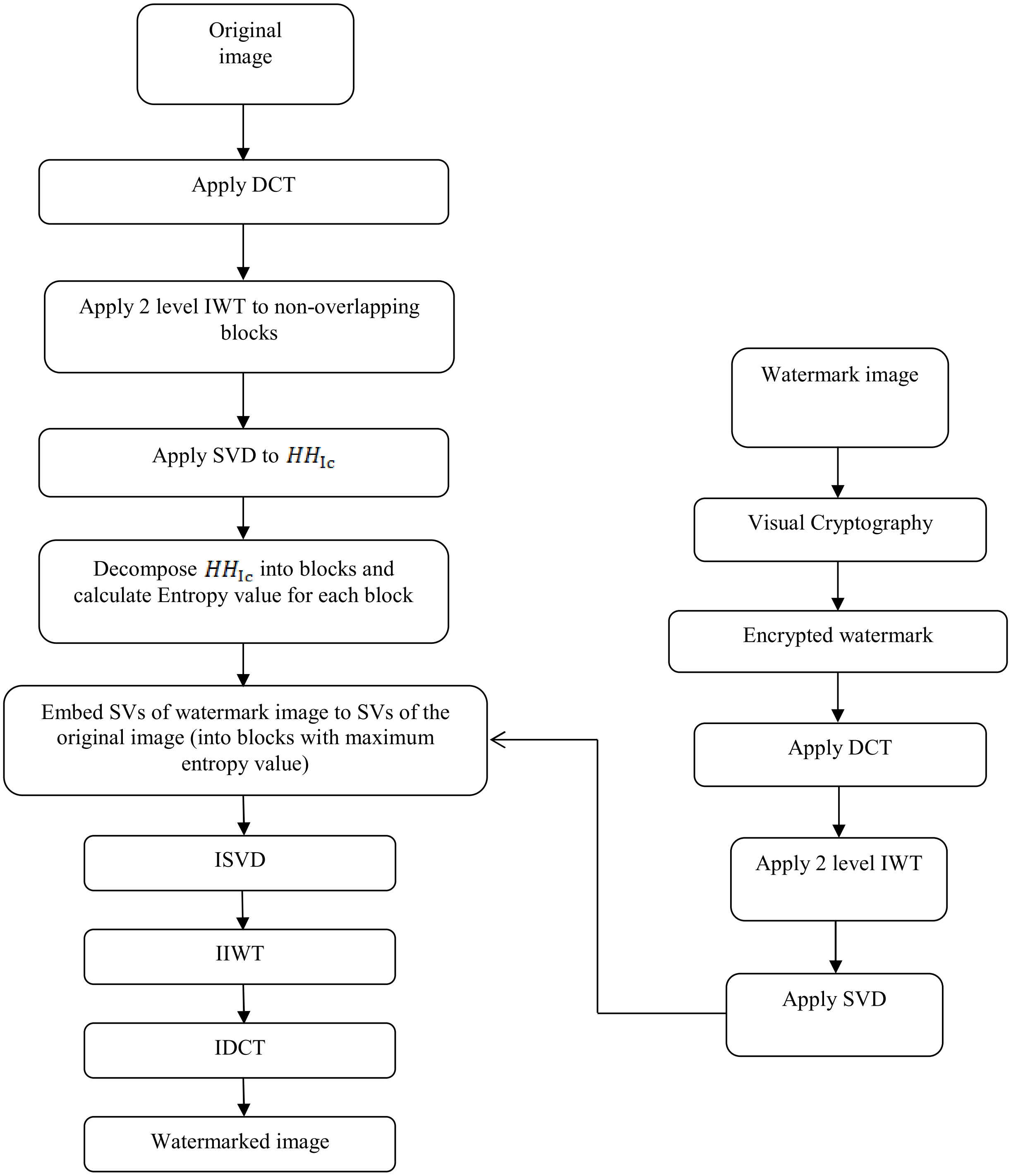

Original image
Apply DCT
Apply 2 level IWT to non-overlapping blocks
Apply SVD to HH_{Ic}
Decompose HH_{Ic} into blocks and calculate Entropy value for each block
Embed SVs of watermark image to SVs of the original image (into blocks with maximum entropy value)
ISVD
IIWT
IDCT
Watermarked image
Watermark image
Visual Cryptography
Encrypted watermark
Apply DCT
Apply 2 level IWT
Apply SVD

Figure 5: Proposed Watermarking Embedding Process

The visual appearance of the watermarked image and the watermark are of very good quality. The metrics used to evaluate the performance of the proposed algorithm are PSNR and SSIM.

PSNR (peak to signal-to-noise ratio) is defined as follows:

$$\mathrm{PSNR} = 10log_{10}\left(\frac{255^2}{MSE}\right)$$

SSIM is utilized to measure the similarity degree between the original watermark and the extracted. Its formula is given below:

$$\mathrm{SSIM} = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu_x{}^2\mu_y{}^2 + c1)(\sigma_x{}^2 + \sigma_y{}^2 + c2)}$$

According to the results of table 1, we can see that our proposed method present the highest value of PSNR and SSIM. Therefore, the distortion of original image is small and the inserted watermark cannot be seen by the human visual system. Hence, we can say that our approach ensures better imperceptibility then the existing methods.

Table 1. Comparison Of Imperceptibility Of Existing Methods

Method	PSNR	SSIM	Watermark type	Watermark size	security
Niu et al	50.31	-	Binary	32x32	-
Kazemi et al	48.81	-	Binary	-	Arnold map
Prabha and Sam	49.20	0.9948	Color	90x90	Shuffling
Sunesh and Kishore	47.66	-	Binary	32x32	-
Wang et al	45.40	0.9872	Binary	64x64	Arnold map
Al Otum et al	62.37	-	Binary	-	Arnold map
Proposed method	**66.42**	**1**	Binary	32x32	Visual Cryptography

5.1 Security test

To enhance security of the proposed watermarking scheme, the watermark image is secured by visual cryptography technique. This technique allows inserting a scrambled watermark in the original image; this prevents the detection of the watermark in clear to remove it or to destroy the quality of the original image. SSIM between the watermark image and the decrypted watermark is 1, which means these two images are identical.

5.2 Imperceptibility anlysis

Imperceptibility represents that the inserted watermark is imperceptible via the human visual system. Imperceptibility is measured in our paper by PSNR and SSIM (Normalized Correlation). These metrics are calculated after the watermark is embedded into the original image.

The proposed method is compared with existing methods in the literature. The results of this comparison are shown in table 1.

Where μ, σ^2, σ_{xy} are mean, variance, and covariance of the images and c1, c2 are the stabilizing constant. SSIM range is from 0 to1. If two images are perfectly matched, SSIM=1.

5.3 Robustness anlysis

With intentional or unintentional modification, Robustness is the fact that the watermarked image retains the inserted watermark. To evaluate the robustness of t he propose approach, several attacks are selected to be performed on the watermarked image. The correlation value between the original watermark and the recovered one is calculated for evaluating the robustness.

$$\mathrm{NC} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n} W(x,y).\tilde{W}(x,y)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} W^2(x,y)\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} W^2(x,y)}}}$$

Where, W (x, y) is the matrix of the original watermark and W̃ (x, y) is the matrix of the extracted watermark.

In table 2, we present PSNR and NC values obtained after applying attacks on Lena, Cameraman, and Jetplane image. Generally, the range of NC is from 0 to 1, it means that the extracted watermark is identical with the original watermark.

Table 2. PSNR And NC Comparison After Different Attack

		Without attack	Salt and paper noise (0.01)	Rotation (20°)	Median filter	Contrast adjustement	Histogram equalization	JPEG QF=70	JPEG QF=50
Lena	PSNR	66.4230	54.7673	50.7857	54.7017	51.2601	52.1675	50.3387	50.3387
	NC	1	1	0.9998	1	1	1	0.9999	1
Cameraman	PSNR	65.0983	41.2546	33.2369	40.2358	40.7789	42.8733	39.3125	38.2368
	NC	1	1	0.9999	1	1	1	1	1
Jetplane	PSNR	64.2652	40.3269	31.3637	40.3187	41.4523	41.8893	38.2548	36.3654
	NC	1	1	0.9999	1	1	1	1	1

On the other hand, the minimum value that the PSNR can have is 30 dB, i.e. the watermarked image has not deteriorated much in quality and the watermark still imperceptible via the human visual system. In our approach, table 2 presents a high PSNR value for the three test images (between 33 dB and 66 dB).

For Lena image the PSNR value is always higher than 50 dB, this means the original image and the watermarked image seem to same from human visual perspective.

In our approach, we have used an encrypted watermark to be inserted in the original image. As shown in table 2, the NC value varies between 0.9998 and 1 for all applied attacks. This indicates that although these attacks were applied, we were able to extract our watermark without any perturbation of its quality. These results show that our proposed method has strong robustness against attacks.

(a) (b)

Salt and pepper noise (0.01)

Different results generated after applying attacks are shown in figure 6.

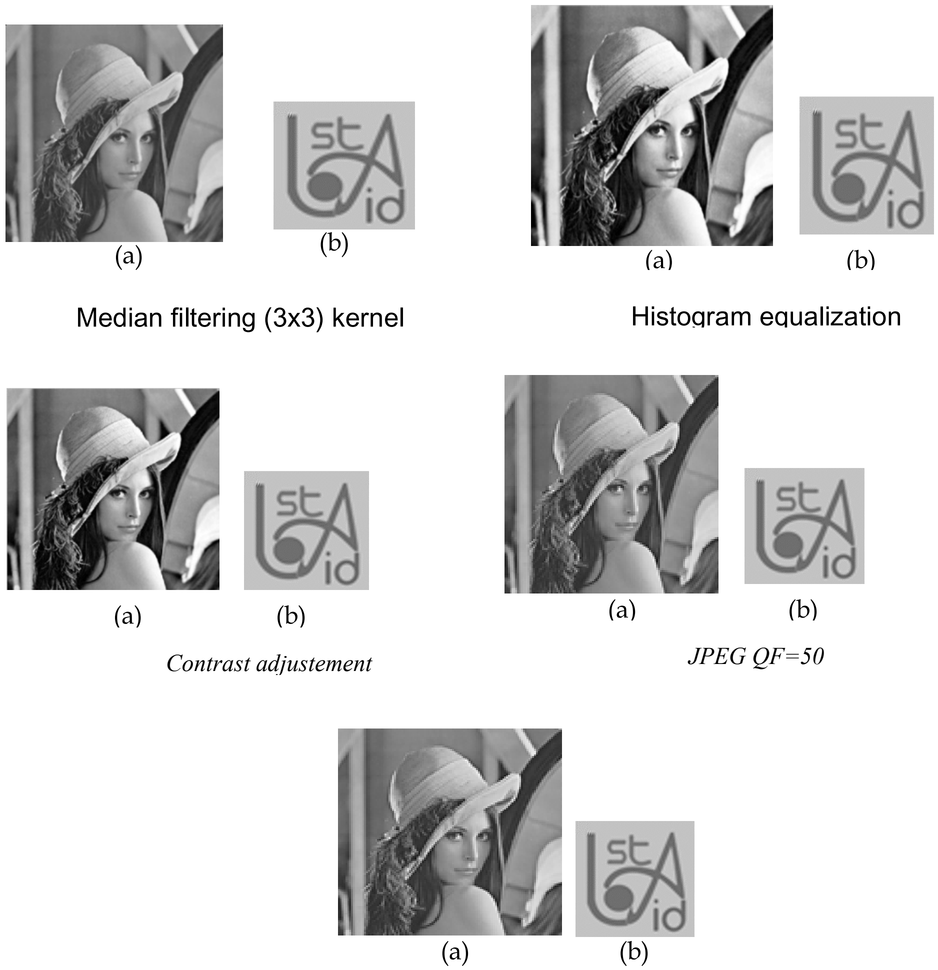
Table 3 compares the robustness of our proposed method with the recent state-of-the-art methods for various attacks by NC.

According to the above comparison results, it is found that the proposed watermarking scheme outperforms the other approaches in terms of invisibility and robustness.

For Cameraman and Jetplane images, we can notice that the PSNR value is higher than 40 dB. This value decreases a little for the JPEG attack but still always higher than 36 dB. For the rotation attack, the PSNR value decreases to 31 dB but does not go fewer than 30 dB. This means that our method still guarantees the imperceptibility criterion. These results show that our proposed method guarantees imperceptibility and robustness against different applied attacks.

(a) (b)

Rotation (20°)



Median filtering (3x3) kernel

Histogram equalization

Contrast adjustement

JPEG QF=50

JPEG QF=70

Figure. 6 watermarked image with extracted watermark under different attacks

Table3. Comparison Of The Robustness Of The Proposed Method With Existing Methods After Attacks By NC

	E Najafi et al 2019 [22]	Rishi Sinhal et al 2021 [35]	Prabha and sam 2020 [35]	Proposed method
Without attack	-	-	-	**1**
Salt and pepper noise (0.01)	0.962	0.994	0.997	**1**
Salt and pepper noise (0.02)	-	0.946	0.993	**1**
Salt and pepper noise (0.05)	0.953	0.789	-	**0.999**
Rotation (10°)	-	-	0.937	**0.999**
Rotation (20^0)	0.990	-	0.892	**0.999**
Rotation (40°)	-	-	0.856	**0.998**
Rotation (50°)	0.990	-	-	**0.998**
Gaussian noise (0.01)	0.956	0.962	-	**1**
Gaussian noise (0.02)	-	0.770	-	**1**
Gaussian noise (0.05)	0.950	0.438	-	**1**
Median filtering (2x2)	-	0.948	-	**1**
Median filtering (3x3)	0.991	0.978	0.837	**1**
Median filtering (5x5)	0.985	-	0.725	**1**
Median filtering (7x7)	0.977	-	0.690	**1**
Median filtering (9x9)	-	-	0.671	**1**
Contrast adjustement	-	-	0.930	**1**
Histogram equalization	0.993	-	-	**1**
JPEG QF=10	0.992	1	-	**1**
JPEG QF=20	0.993	1	-	**0.999**
JPEG QF=30	0.993	0.986	-	**0.998**
JPEG QF=40	0.993	0.944	-	**0.997**
JPEG QF=70	0.993	-	-	**0.995**

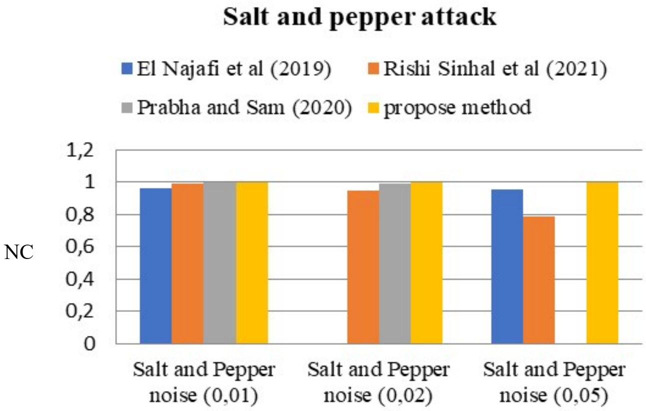


Figure 7. NC Of Salt And Pepper Attack

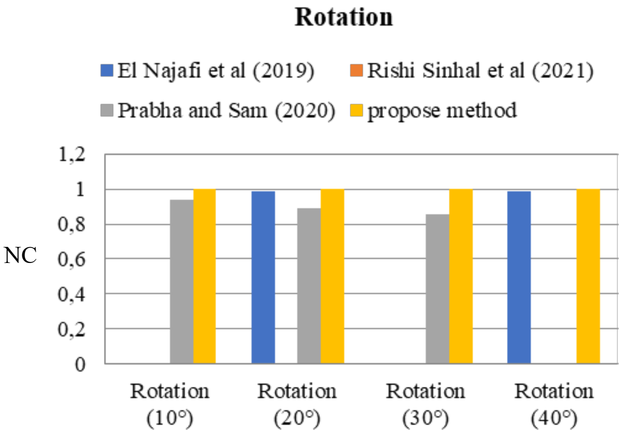


Figure 8. NC of Rotation Attack

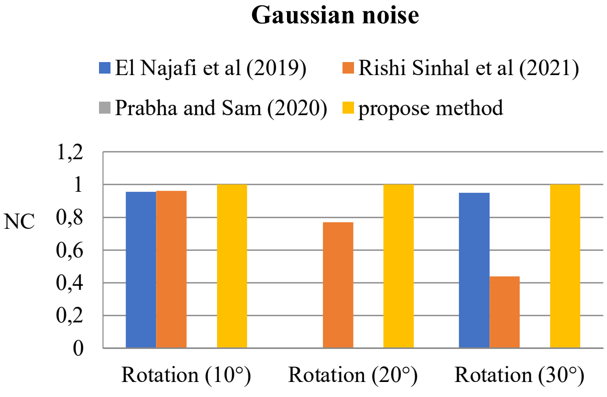


Figure 9. NC of Gaussian Noise Attack

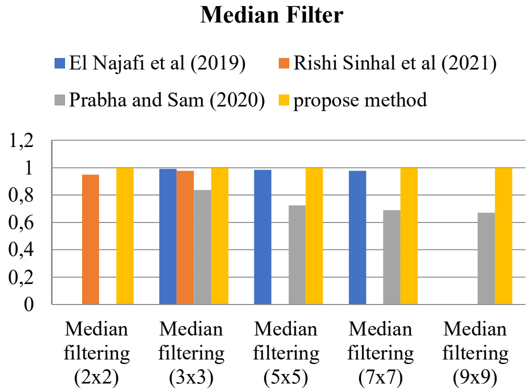


Figure 10. NC of Median Filter

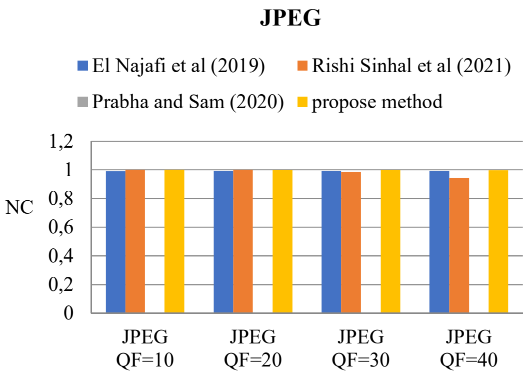


Figure 11. NC of JPEG

From these figures, different attacks are presented to test the robustness of the watermarking scheme such as, salt and pepper, rotation, Gaussian noise, median filter and JPEG attacks. We can notice that the NC values of our proposed method are higher than the existing methods in the literature. Generally, the NC values varies between 0.95 and 1. Hence, the robustness of extracted watermark without affecting the imperceptibility of original image is improved and therefore, the robustness of this scheme is high.

6. THREATS OF VALIDITY

This section presents the threats of validity of this paper with respect to internal, external and constructs validity.

Internal validity: This paper uses the maximum entropy like a feature selection that select the optimal blocks suitable for the watermark process to have robustness and a good imperceptibility of the method.

External validity: This study uses some test image to validate the watermarking process. However, we can use other different test image to test the efficacy of our proposed method in a large database. Also, we can suggest the fusion of other decomposition techniques to ameliorate the performance results.

Construct validity: This study focused on the use of NC, PSNR and SSIM to evaluate the performance of our method in terms of robustness and imperceptibility with different attacks. The main reason behind this choice is that the most of the studies used them to measure the performance of their methods.

7. CONCLUSION

By combining 2-level IWT with SVD and DCT, a multi-scale watermarking is proposed in this study. We have proposed a robust and efficient watermarking method for copyright protection. A watermark embedding and extraction algorithm is implemented. Different Evaluation of the proposed method is presented. PSNR, SSIM and NC parameters are compared to the existing method in the literature. The experimental results show that this method is robust against most attacks. We obtained NC =1; which means that we have a great similarity with watermark and extracted watermark. Visual cryptography provides enhanced security to the proposed method. Thereby we can conclude that our method ensure the four basic requirement of watermarking (imperceptibility, robustness, security and large capacity). Despite these results, our method knows limitations in terms of execution time and implementation of a single watermark for the embedding algorithm instead of several. Multiple watermark provide better against different image manipulation. The future work will focus on digital watermarking based on machine learning and deep learning model. In addition, this work can be extended by combining various techniques in different domains with CNN architectures by changing grayscale images by color images.

REFERENCES:

[1] Ambadekar, Sarita P., Jayshree Jain, and Jayshree Khanapuri. "Digital image watermarking through encryption and DWT for copyright protection." Recent Trends in Signal and Image Processing. Springer, Singapore, 2019. 187-195.

[2] Liu, Yang, et al. "Secure and robust digital image watermarking scheme using logistic and RSA encryption." Expert Systems with Applications 97 (2018): 95-105.

[3] Jafar, Iyad F., et al. "An efficient reversible data hiding algorithm using two steganographic images." Signal Processing 128 (2016): 98-109.

[4] Al-Afandy, Khalid A., et al. "High security data hiding using image cropping and LSB least significant bit steganography."2016 4th IEEE International Colloquium on Information Science and Technology (CiSt). IEEE, 2016.

[5] Zhou, Xinyi, et al. "An improved method for LSB based color image steganography combined with cryptography." 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS). IEEE, 2016.

[6] Singh, Durgesh, and Sanjay K. Singh. "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection." Multimedia Tools and Applications 76.11 (2017): 13001-13024.

[7] Rani, Asha, and Balasubramanian Raman. "An image copyright protection scheme by encrypting secret data with the host image." Multimedia Tools and Applications 75.2 (2016): 1027-1042.

[8] Divya et al" 3D Image Watermarking And Quality Assessment" International Journal Of Scientific & Technology Research, Volume 8, Issue 11 (2019).

[9] Arezoo Nouri Heydarlo, et al. "The Secure Watermarking Of Digital Color Images By Using A Combination Of Chaotic Mapping" International Journal Of Scientific & Technology Research, Volume 6, Issue 6 (2019).

[10] Deeba, Farah, et al. "Protecting the Intellectual Properties of Digital Watermark Using Deep Neural Network." 2019 4th International

Conference on Information Systems Engineering (ICISE). IEEE, 2019.

[11] Yu, Chong. "Steganography of Digital Watermark Based on Artificial Neural Networks in Image Communication and Intellectual Property Protection." Neural Processing Letters 44.2 (2016): 307-316.

[12] Zhang, Jialong, et al. "Protecting intellectual property of deep neural networks with watermarking." Proceedings of the 2018 on Asia Conference on Computer and Communications Security. 2018.

[13]ZHANG, Xueting, SU, Qingtang, YUAN, Zihan, et al. An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform. Optik, 2020, vol. 219, p. 165272.

[14] YUAN, Zihan, SU, Qingtang, LIU, Decheng, et al. Fast and robust image watermarking method in the spatial domain. IET Image Processing, 2020, vol. 14, no 15, p. 3829-3838.

[15] ELBASI, Ersin et KAYA, Volkan. Robust medical image watermarking using frequency domain and least significant bits algorithms. In : 2018 International Conference on Computing Sciences and Engineering (ICCSE). IEEE, 2018. p. 1-5.

[16] LI, Meng, ZHONG, Qi, ZHANG, Leo Yu, et al. Protecting the intellectual property of deep neural networks with watermarking: The frequency domain approach. In : 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020. p. 402-409.

[17] RAKHEJA, Pankaj, VIG, Rekha, et SINGH, Phool. An asymmetric watermarking scheme based on random decomposition in hybrid multi-resolution wavelet domain using 3D Lorenz chaotic system. Optik, 2019, vol. 198, p. 163289.

[18] RAKHEJA, Pankaj, SINGH, Phool, et VIG, Rekha. An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain. Optics and Lasers in Engineering, 2020, vol. 134, p. 106177.

[19] VENKATESH, S. et DORAIRANGASWAMY, M. A. Implementing Efficient Audio and Image Watermarking Using Multi-resolution Dual Wavelet and Fireflies Approach in Wireless Network. Wireless Personal Communications, 2018, vol. 102, no 4, p. 2389-2401.

[20bis] TIAN, Cheng, WEN, Ru-Hong, ZOU, Wei-Ping, et al. Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain. Multimedia Tools and Applications, 2020, vol. 79, no 11, p. 7515-7541.

[21] Ansari, Irshad Ahmad, and Millie Pant. "Multipurpose image watermarking in the domain of DWT based on SVD and ABC." Pattern Recognition Letters 94 (2017): 228-236.

[22] Najafi, Esmaeil, and Khaled Loukhaoukha. "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform." Journal of information security and applications 44 (2019): 144-156.

[23] Madhavan, Sundararajan, and Govindarajan Yamuna. "DWT-based grey-scale image watermarking using area of best fit equation and cuckoo search algorithm" International Journal of Computational Science and Engineering 15.3-4 (2017): 236-247.

[24] MOHAMED RADOUANE, TARIK BOUJIHA, ROCHDI MESSOUSSI, RAJA TOUAHNI, “A ROBUST METHOD FOR DIGITAL IMAGES WATERMARKING BASED ON COMBINATION OF SVD, DWT AND DCT USING OPTIMAL BLOCK”, JATIT, 2013.

[25] ZHANG, Yifeng, LI, Yingying, et SUN, Yibo. Digital watermarking based on joint DWT–DCT and OMP reconstruction. Circuits, Systems, and Signal Processing, 2019, vol. 38, no 11, p. 5135-5148.

[26] ZHENG, Peijia et ZHANG, Yonghong. A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks. Multimedia Tools and Applications, 2020, vol. 79, no 25, p. 18343-18365.

[27] AL-OTUM, Hazem Munawer. Secure and robust host-adapted color image watermarking using inter-layered wavelet-packets. Journal of Visual Communication and Image Representation, 2020, vol. 66, p. 102726.

[28] SINGH, Rajiv, NIGAM, Swati, SINGH, Amit Kumar, et al. Integration of wavelet transforms for single and multiple image watermarking. In : Intelligent Wavelet Based Techniques for Advanced Multimedia Applications. Springer, Cham, 2020. p. 51-63.

[29] PRABHA, K. et SAM, I. Shatheesh. An effective robust and imperceptible blind color image watermarking using WHT. Journal of

King Saud University-Computer and Information Sciences, 2020.

[30] Winarno, Agus, et al. "Image watermarking using low wavelet subband based on 8× 8 sub-block DCT." 2017 International Seminar on Application for Technology of Information and Communication (iSemantic). IEEE, 2017.

[31] Makbol, Nasrin M., Bee Ee Khoo, and Taha H. Rassem. "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics." IET Image processing 10.1 (2016): 34-52.

[32] Thakkar, Falgun N., and Vinay Kumar Srivastava. "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications." Multimedia Tools and Applications 76.3 (2017): 3669-3697.

[33]ZAINOL, Zurinahni, TEH, Je Sen, ALAWIDA, Moatsum, et al. A new chaotic image watermarking scheme based on SVD and IWT. IEEE Access, 2020, vol. 8, p. 43391-43406.

[34] ALOTAIBI, Reem A. et ELREFAEI, Lamiaa A. Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). Applied Computing and Informatics, 2019, vol. 15, no 2, p. 191-202.

[35] SINHAL, Rishi, JAIN, Deepak Kumar, et ANSARI, Irshad Ahmad. Machine learning based blind color image watermarking scheme for copyright protection. Pattern Recognition Letters, 2021, vol. 145, p. 171-177.

[36] PRABHA, K. et SAM, I. Shatheesh. An effective robust and imperceptible blind color image watermarking using WHT. Journal of King Saud University-Computer and Information Sciences, 2020.