



A Novel Color Image Watermarking Method based on Digital Wavelet Transform and Hungarian Algorithms

Amir Hesam Yaribakht¹, Mohd Shahidan Abdullah², Alireza Ghobadi³

¹Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia, hyamir2@live.utm.my

²Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia, mshahidan@utm.my

³SOHA Sdn Bhd, Malaysia, ghobadi@soha.com.my

ABSTRACT

In the last few years, high data growth rate has funded the new outlook of ecommerce like electronically marketing, publishing, transmission and distribution of real time multimedia data in the form of video, audio, image and so on. Unauthorized access and copyright protection become a vital concern for almost all of the digital data service providers. In the past ten years, many researchers proposed various methods such as steganography, cryptography, watermarking and so on for different purposes [1]. Watermarking is proposed to protect digital data against unauthorized activities and help to maintain copyright ownership by embedding watermark data into host signal using some modification in its content [2], [3]. The effectiveness of a digital watermarking depends on the few characteristics such as imperceptibility, robustness, security, and real-time processing [4]. Many researches have been done one gray scale image compare to color image because color image redundant data cannot be used sufficiently and cause poor ability to resist attacks which means the method has low robustness against image processing attacks [5]. This paper proposed a new DWT-Hungarian method for color image watermarking to overcome this problem and the experimental results show that the proposed method has high robustness against JPEG (30) compression, cropping (50%), scaling, rotation and blurring attacks than other related works.

Key words : Color image watermarking, DWT, Hungarian Algorithm, Robustness.

1. INTRODUCTION

In the past few years, high data growth rate has funded the new outlook of ecommerce like electronically marketing, publishing, transmission and distribution of real time multimedia data in the form of video, audio, image and so on. Although there are numerous advantages for multimedia contents to be digitized compared to analog equivalent, the service providers are too careful to offer the services in their digital structure because of concerning of freely copy and distribution of copyright resources. Over the last decade, various methods proposed by researchers to protect

multimedia data and digital watermarking methods are better compared to other methods like steganography, cryptography, and others [1].

On the other hand, unauthorized access becomes vulnerability of digital data because digital data can be distributed everywhere by widespread of transmission medium. Thus, to protect digital data an intellectual property considers extra attention on them. One of the optimistic methods to protect digital data copyright is digital watermarking. The watermark in digital watermarking is an identity code that carries data about the work inventor, the ownership copyright, legal customer and so on [2]. Watermarks are used to keep safe digital media from unauthorized use, piracy and any other illegal actions. In watermarking method watermark data is embedded into host signal by some modification of its content [3].

Moreover, fast development of multimedia technology and internet arise many problems for digital data such as illegal modifying of digital copyright, tampering and copying. Therefore, many methods such as digital watermarking have been proposed to address these problems and maintain information safety. The effectiveness of a digital watermarking depends on the following characteristics [4]:

- **Imperceptibility:** The watermark needs to be invisible or inaudible in watermarked “image/video” or “digital music” respectively. Human perception must be maintained about host object after extra data (watermark) has been embedded in it. Imperceptibility evaluation is normally based on a subjective test with specified procedures or an objective measure of quality, which is called Peak Signal-to-Noise Ratio (PSNR) [4].
- **Robustness:** Unauthorized distributors should not be able to eliminate or remove the embedded watermark by using common image processing operations such as cropping, compression, quantization and filtering [4].
- **Security:** To ensure security, watermarking procedure should depend on secret keys, so that attacker could not be able to remove or detect watermark by statistical analysis from a set of multimedia files or images. An unauthorized user who may even have a prior knowledge of the exact watermarking algorithm, cannot sense the existence of hidden data, without having the secret keys which have been used in the embedding procedure [4].
- **Real-time processing:** Embedding procedure must be fast and without having any delay, watermark should be quickly embedded into the host object [4].

Furthermore, these days with rapid development of internet and mobile devices, digital images can be easily captured and stored everywhere. Also, they can be shared on popular social media like Instagram, Twitter, Facebook and so on [6]. Wireless communication channels are normally used to upload these images to the internet directly without having any primary protection schemes [7]. This causes numerous urgent issues relating to copyright protection and authentication in transmission, storage, and usage of images. For instance, a personal image which has been shared on a social media can be illegally accessed, downloaded, modified, and reused by others for some intentions like commercial or other purposes [6].

To summarize, most of the researchers works on gray scale image based on copyright protection and authentication. A few researchers work on color image and most of these color image watermarking methods use only one-color channel or each color channel of a color image to embed the watermark data. So, the color image's redundant data cannot be used sufficiently and cause poor ability to resist attacks which means the method has low robustness against image processing attacks [5].

In this paper, fifteen research papers have been reviewed and only five of them which used the same image size from the same image databased and watermark image, used to compare with the proposed method. This paper focused on color image watermarking only. The purpose of this paper is to analysis of recent five years' researchers' methods and compare their results on color image watermarking with the proposed method. The new method result has been compared with other relate works' results. The paper structured to categories the watermarking methods and compare them based on the five attacks' results (JPEG (30) compression, cropping (50%), scaling, rotation and blurring) followed by explanations of the new proposed methods in detail. At the end, explain future work for this research.

2. RELATED WORKS

Since 2001, there are number of works related to digital color image watermarking. This section describes the most recently fifteen papers related to novel methodologies for color image watermarking between years 2013 until 2017. Table 1 indicates the comparison of these fifteen related papers [1], [2], [3], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] based on their methods and attacks. Five of the most related papers to this research has been summarized as below. Su, et al. [8] proposed a blind double color image-watermarking algorithm based on QR decomposition. In this research in embedding process, the color host image, which is 24 bits with size of 512×512 , is divided into 4×4 distinct pixel blocks and QR is used to decompose each pixel block. Then, according to similarity between the 2nd row 1st column and the 3rd row 1st column coefficient in original matrix Q, the color watermark image which is 24 bits with size of 32×32 is embedded into the host image. Furthermore, to improve the imperceptibility of watermark, compensatory method is used in the matrix R. The Arnold transform and the

MD5 algorithm with different private keys are used to enhance the watermark security. In watermark extraction process, neither original image nor watermark image is needed. No false-positive problem and the simplicity of the proposed method compared to other SVD-based method are the two advantages of this method. This method only needs 1.481403 second to run. The experimental results indicate that proposed method compared with some researchers' methods has better watermark invisibility and stronger robustness against JPEG2000 compression, JPEG compression, cropping, low pass filtering, rotation, adding noise, scaling, blurring and sharpening.

Su, et al. [9] proposed color image blind watermarking scheme based on QR decomposition. This research stated that the majority of the existing color image watermarking methods are non-blind watermarking methods and gray scale or binary image have been used as watermark. On the other hand, designing a blind color image watermarking method is a challenging problem. The purpose of this research is to use QR decomposition to propose a blind color image watermarking method to embed color image as a watermark into color host image. In the first step, 4×4 distinct pixel blocks are created by dividing the color host image. Then, QR decomposition is used to decompose each selected pixel block and, in the matrix, R the 1st row 4th column element is quantified for embedding the watermark information. In extraction process, the watermark can be extracted without any need to have original host image or watermark image. The experimental results indicate that the proposed method has higher watermark invisibility and stronger robustness against almost all common attacks like cropping, noise adding, compression, scaling, blurring, sharpening, filtering and etc. Su and Chen [10] proposed an improved color image watermarking scheme based on Schur decomposition. From Schur decomposition, the 4×4 unitary matrix U and the upper triangular matrix D is analyzed and the embedding column c of matrix U is decided by the matrix D's maximum eigenvalue column; moreover, it is found that there is strong similarity between the entries of the 2nd row the cth column and the 3rd row the cth column in the matrix U. The novelty of the proposed method is to use these properties to embed and blindly extract the watermark from the different attacked images and also use color image as watermark. Experimental results indicate that the proposed method has better invisibility, stronger robustness against common image processing and geometric attacks, higher capacity and security, better computational complexity, etc., compared with other proposed methods. The Schur-based method has better watermark performance compare with QR-based, SVD-based and spatial domain algorithms.

Su, et al. [11] proposed a new algorithm of blind color image watermarking based on LU decomposition. The watermark invisibility enhanced because of the higher similarity of 1st column the 2nd row element and the 1st column the 3rd row element of the lower triangular matrix which achieved by LU decomposition and by slightly modifying rules, the color image watermark can be embedded into these elements.

Further, to improve the watermark security, Arnold transform is used and to improve the watermark robustness, the Hash pseudo-random number algorithm based on MD5 is used. In the extraction process, to extract the watermark from the attacked watermarked image, need to have the watermark embedding strength and private key. There is no need to have original watermark image or the host image to extract the watermark, which mean the proposed method, is blind. Experimental results indicated that the proposed method has higher invisibility, stronger robustness against most common image processing attacks such as JPEG compression, JPEG 2000, salt and pepper noise, Gaussian noise, Median filter, low-pass filter, sharpening, blurring, scaling and cropping attacks and furthermore, it has high embedding payload and computational complexity, compare to other researches' methods.

Su and Chen [12] proposed a novel blind color image watermarking using upper Hessenberg matrix. To improve the proposed method's security, Arnold transform is used and to

improve its robustness, the MD5-based Hash pseudo-random algorithm is used. In the watermark embedding process, quantization technique is used to embed the encrypted color watermark image information into the maximum element in the upper Hessenberg matrix by modifying the biggest energy element. In the watermark extraction process, the watermark is blindly extracted from attacked watermarked image, which means that, there is no need to have original watermark image or original host image to extract the watermark. Experimental results indicate that the proposed method has better invisibility, stronger robustness against most common image processing attack like JPEG compression, JPEG 2000, salt and pepper noise, Gaussian noise, Median filter, low-pass filter, sharpening, blurring, scaling and cropping attacks and also it has high capacity and computational complexity, compare to other researches' methods.

Table 1 shows other researchers' methods and their Normalized Cross-Correlation (NCC) which measure the robustness against attacks.

Table 1: Papers' Methods and Its NCC Results after Attacks

Ref No.	Methods	Watermarking Attacks									
		Filter		Noise		JPEG Compression	Scaling	Rotation	Cropping	Blurring	Sharpening
		Median	Low pass	Salt & Pepper	Gaussian						
[1]	DWT, USC-ABC	0.67	-	0.89	0.80	0.80	0.96	-	0.75	-	-
[2]	Arnold transformation, SVD	0.98	-	0.95	0.99	0.95	-	-	-	0.98	-
[3]	DWT, QR decomposition, CZT, SVD	-	-	0.96	0.93	0.87	0.94	-	0.93	0.98	0.99
[8]	Arnold transformation, Private Key, MD5, QR decomposition	0.35	0.86	0.96	0.69	0.89	0.89	-	0.77	0.88	1.00
[9]	Arnold transformation, Private Key, MD5, QR decomposition	0.99	0.92	0.83	0.92	0.95	0.99	-	0.75	0.83	0.99
[10]	Arnold transformation, Private Key, Schur Decomposition	0.73	0.93	0.89	0.85	0.93	0.94	-	0.66	0.94	1.00
[11]	Arnold transformation, Private Key, MD5, LU decomposition	0.92	0.96	0.98	0.89	0.96	0.99	-	0.85	1.00	0.99
[12]	Arnold transformation, Private Key, MD5, Hessenberg decomposition	0.96	0.97	0.97	0.96	0.95	0.99	-	0.63	1.00	0.99
[13]	Arnold transformation, SVD	0.80	0.89	0.98	0.88	0.87	0.97	-	0.87	0.63	0.81
[14]	Arnold transformation, DC Coefficient	0.95	-	0.93	0.96	0.98	0.90	0.79	0.93	-	-
[15]	DCT, AC Coefficient, DC Coefficient, YIQ color transformation	0.91	0.99	0.98	-	0.99	-	0.83	0.97	-	0.99
[16]	QDFT, IULPM, Arnold transformation, Private Key	0.87	-	0.94	0.85	0.80	0.95	0.73	0.98	-	-
[17]	DWT, SVD	0.94	-	0.99	1.00	0.96	-	0.94	0.94	-	-
[18]	MD5, Hessenberg decomposition, Contourlet transform	0.85	-	0.86	-	0.85	0.97	-	0.87	-	-
[19]	DWT, Arnold transformation, SVD	0.99	-	0.99	0.99	0.99	-	0.99	0.99	0.99	0.99

3. SOME COMMON MISTAKES

In general, watermarking method needs two pre-processing. First is to find Region of Interest (ROI). This process helps to find the best place in host image for embedding the watermark. Second, is to find the best method to embed watermark to host. The embedding happens in the place,

which has been determined by ROI process. Most of the existing watermarking methods do not determine the ROI which means that the whole host image is used as ROI by default.

This research proposed a novel DWT-Hungarian color image watermarking method based on define both process, which explain previously. The fundamental problem in watermarking is to find the right place for embedding

purposes that has the least effect on the host image quality. This research uses Hungarian algorithm to find the optimum embedding places in the host image. Then using DWT scheme to embed the color image watermark into the second level of DWT LL2.

Figure 1 shows a block diagram of a general scheme for the proposed method in this paper. This includes: (i) ROI detection stage (described in Section A.); (ii) Embedding watermark in host by using DWT; (iii) Extraction stage, which shows extraction method for retrieving the watermark image.

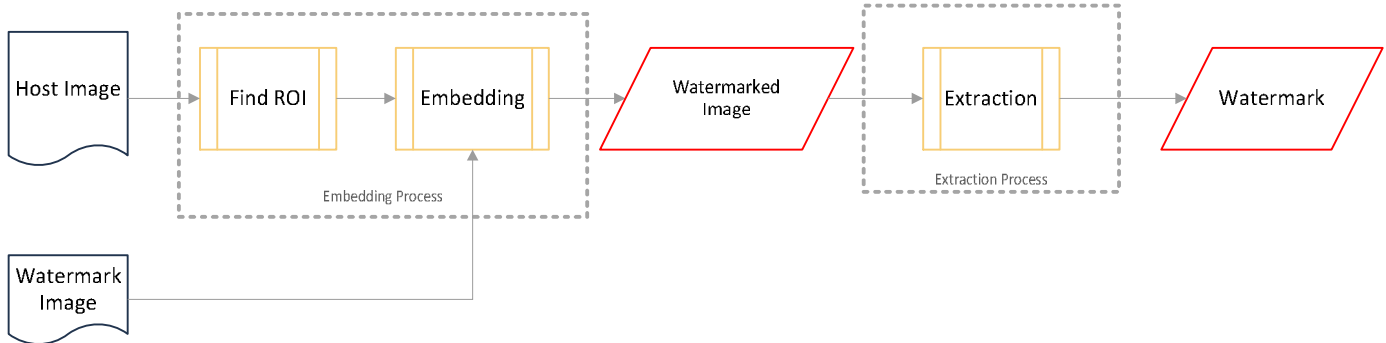


Figure 1: General Scheme for the Proposed Method

3.1 Find Region of Interest (ROI) Process

In the proposed method, Hungarian algorithm is used to find ROI in host image, which normally used for assignment problem. The Hungarian algorithm which has been previously described by Kuhn’s Hungarian algorithm [20] defined as below.

A. Hungarian Methods

Hungarian method uses to answer, “How to assign M jobs when N workers are available?” The idea is to find the combination the results in the least possible cost. Imagine that you have two workers and two jobs where each worker has a different cost to do each job. So, there are four combinations to be considered and the intention is to find the least possible cost combination. When the number of workers and jobs increased, such a problem grows exponentially which make it impossible to consider each combination every time. This problem is recognized as assignment problem and without the problem being optimized, to reach at the solution, n! trials need to be conducted. To solve the assignment problem, the fastest way is to use Kuhn’s Hungarian algorithm [20] to find a solution in polynomial time [21].

The Hungarian algorithm steps are as follow and Fig. 2 indicate an example of it [21]:

- Step 1: Subtract in row: Find the minimum value in each row and then deduct it from all entries in the same row. Therefore, there is at least one zero entry value in each row of the matrix. Noted that all entries of the matrix are positive numbers.
- Step 2: Subtract in column: Deduct the minimum column value from all entries on that column. Therefore, there is at least one zero value in all the columns and rows of the matrix. Noted that all entries of the matrix are positive numbers.
- Step 3: Use minimum lines to draw across the columns and rows in such a way that all the zeros in the matrix are covered.

Step 4: The optimality test is completed when the number of drawn lines is equal to n, nevertheless if it is lower than n, we need to continue with step 5.

Step 5: From the uncovered entry values find the smallest entry and then add it to those entries that are covered twice and deduct it from every uncovered entry. Then go back to Step 3.

Note: There is a possibility that two distinct assignment provide the similar total minimum cost value [21].

As it can be seen, Figure 2 shows an example of Hungarian Algorithm using 4×4 matrix [22].

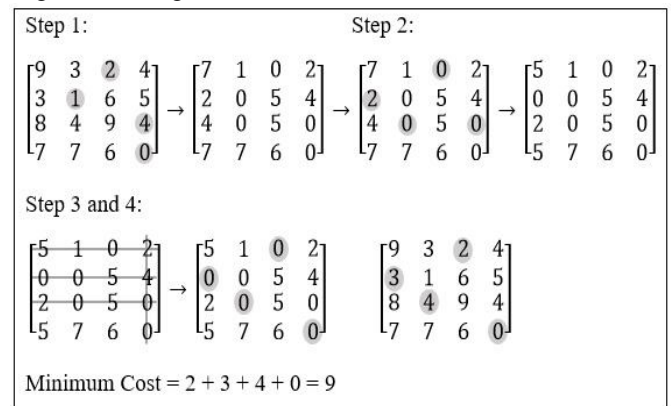


Figure 2: Hungarian Algorithm Example [22]

This ROI method is proposed to identify the best embedding place in host image. To find this area Hungarian algorithm is used, which will be explained in the next section. The method was tested against different host and watermark. This paper uses 24-bits 512×512 color host image from CVG-UGR image database and 24-bits 32×32 color watermark image (Peugeot logo). The embedding method involves several steps: (i) the original RGB host is divided to R, G and B Matrix; (ii) Do Hungarian process for each matrix; (iii) Provide sub matrix of each color matrix based on divided counter value (which is private key) and calculate number of the zero for each sub matrix and store; Find sub matrix which

include maximum value of zero; (v) Choose that submatrix as ROI area; Embed watermark by DWT level2 in that area; and (vii) Combine ROI watermarked with original host.

B. Discrete Wavelet Transforms (DWT)

This is a relatively new method which has been used to support various digital media activities including watermarking. These transforms are made up of small waves called wavelets which vary in frequency and duration. This transform breaks the image down into three spatial directions, i.e. horizontal, vertical and diagonal and that is the reason they tend to represent the characteristics of HVS more closely. The size of DWT coefficients is higher in the lowest bands and lower in the higher bands. Many applications that processes signal such as noise removal, audio and video compressing and so on make use of DWT. Wavelets are more time focused and are therefore useful tools in analyzing transient signals that vary in time. Many of the real signals tend to be time-varying by nature and therefore the wavelet transform is suitable for numerous applications. However, one of the biggest challenges for watermarks is to find the right balance between robustness and imperceptibility. This is because, when you try to increase the robustness of the image, the level of distortion also increases. Nevertheless, DWT is more preferred as compared to other as it spreads the frequency of the watermark and facilitates a spatial localization at the same time within the image. The basis of DWT is to break the image into sub images of varying spatial and frequency domains [23], [24].

Furthermore, the wavelet transform indicates a development process for decomposition of a specified signal on the basis of orthogonal functions. DWT is efficient to deal with advanced problems because it has ability to provide both frequency and location information of the analyzed signal. DWT decomposition (figure 3) is used to generate four distinct sub-bands which are non-overlapping multi-resolution. As it can be seen in Fig. 3, these sub-bands are: LL (Approximate sub-band), HL (Horizontal sub-band), LH (Vertical sub-band) and HH (Diagonal sub-band) [25].

LL1	HL1
LH1	HH1

Figure 3: DWT decomposition [26]

C. ROI Concept

Region of Interest (ROI) is one of the considerations in watermarking. The proposed method used combination of the basic concept of coloring and Hungarian algorithm to find the best embedding places from the host image to embed the color watermark image.

The basic concept of Hungarian algorithm is to find the minimum entry value of the row (or column) and deducted from the same row (or column) of the matrix. With this way, at least one entry value become zero in row (or column) of the

matrix. The zero entry values show the best locations in the host image matrix to hide the watermark information in them randomly.

One way is to use all of the zero entry values to hide the watermark information. On the other hand, the watermark matrix size can be calculated and then match them with zero entry values from the host image which is calculated by Hungarian algorithm. The proposed method uses a private key to save the embedded locations in host image matrix for the extraction purpose.

The novelty of the proposed method is to create number of sub-images from host image then calculate zero entry values in all sub-images' matrix, after that find the sub-image matrix with the maximum zero entry value in it.

In addition, let's make an example to make it easy to understand. We choose Lena image as host with size of 512x512 pixels (24-bits). Then the host matrix is $H_{512 \times 512}$ with below definition:

$$H_{m \times n} = \sum_{i=0}^m \sum_{j=0}^n h_{i \times j} \quad \text{Where } m = 512 \text{ AND } n = 512 \quad (1)$$

$$\forall x \in \mathbb{N} : 0 \leq x \leq m \quad \text{AND} \quad \forall y \in \mathbb{N} : 0 \leq y \leq n \quad (2)$$

$$SH_{k \times l} = \sum_{i=0}^k \sum_{j=0}^l h_{i \times j} \quad \text{Where } k = m - x \text{ AND } l = n - y \quad (3)$$

Equations (1), (2), and (3) mathematically defines host image and sub host images. Sub host images has been created based on the x and y value. Figure 4 shows the host image and sub host images.

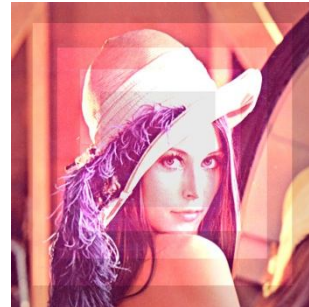


Figure 4: Host Image and Sub-host Images

To find ROI area, ratio of zero population in each sub host image has to be calculated. The equation of ration calculation is defined based on (4).

$$\sum_{i=0}^n R_i = z / (k \times l) \quad \text{Where } \forall z \in \mathbb{N} : 0 < z < n \quad (4)$$

The ROI, which has been chosen, is a maximum number of R_i . Figure 5 shows the chosen area.



Figure 5: Selected Area as ROI Region

The next steps are to use one of the watermarking methods to embed watermark in the ROI area. The proposed method,

which is used for this experience is DWT level2. Based on DWT level 2 explanation [22], the method is robust. After embedding the watermark in sub host image, the sub image returns to the position on the original host image. The private key shows the R_i (ROI) in the host image.

3.2 Embedding Techniques

The embedding processes (figure 6) for the proposed method are as below:

1. Host image is divided to RGB color channel;
2. Hungarian algorithm is used to find minimum pixel value and calculate the number of zero-pixel value in each RGB color channel;

3. By using counter number, create a region of interest from host image and calculate number of zero in this area for each RGB color channel;
4. Calculate the maximum zero-pixel value and then select a region area for watermark embedding and generate the private key by using counter number;
5. Using 2-level DWT to embed the color watermark into the LL2 in the selected area;
6. Return the selected area into the host image after embedding process is finished.

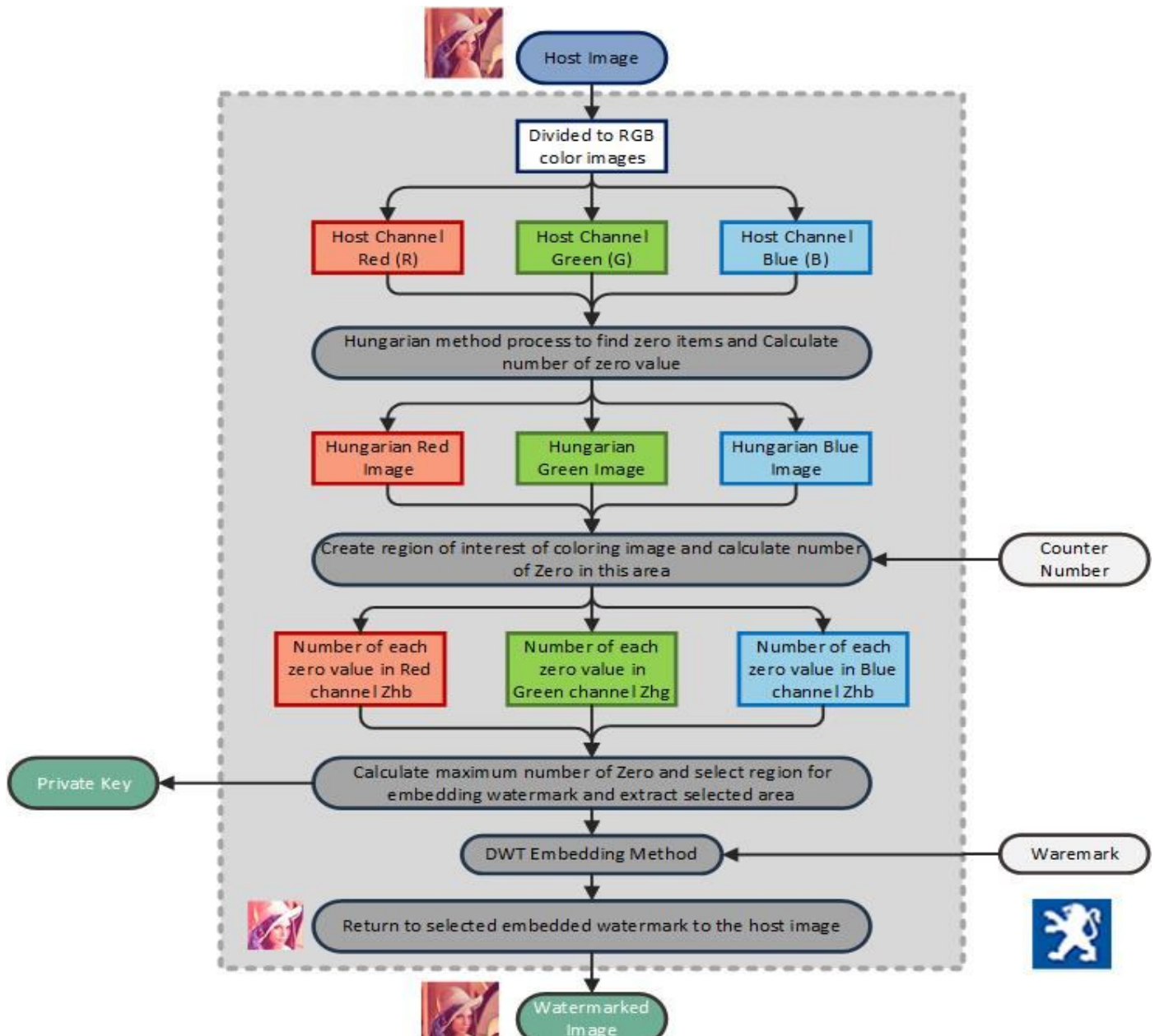


Figure 6: Embedding process

3.3 Extraction Techniques

One of the novelties of the proposed method is its simplicity. This section explains how to extract watermark from watermarked image. As it can be seen in Figure 7, the extraction technique involves few steps as below:

1. Use the private key (created by using counter number);
2. Extract sub image from watermarked image;
3. Reverse DWT level 2 by using IDWT.

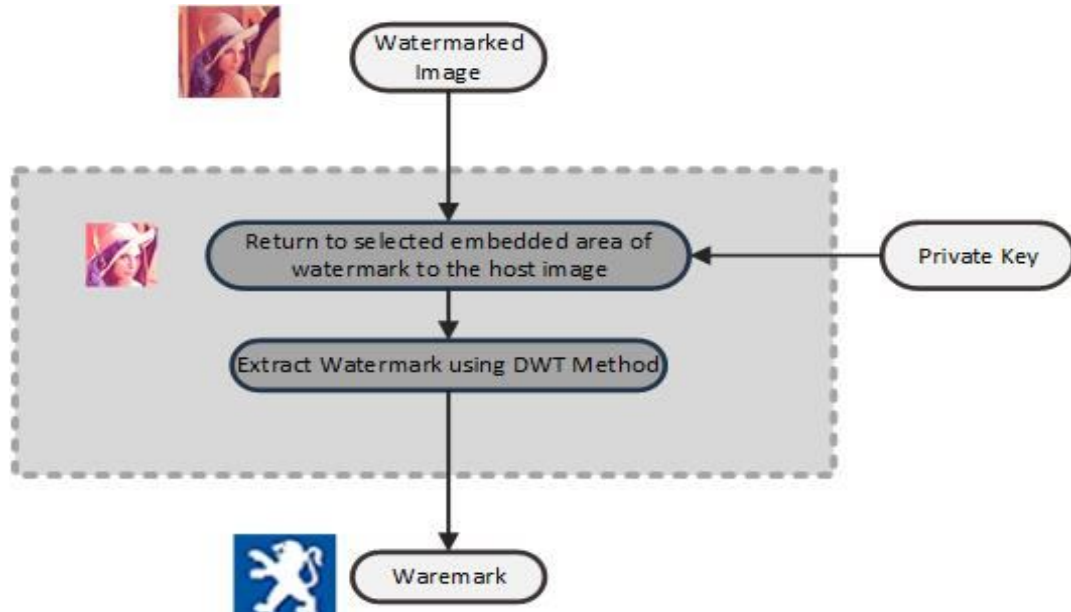


Figure 7: Extraction process

3.4 Security Analysis

This section analyzes the security of the proposed DWT-Hungarian embedding method. First, investigate the robustness of the generated random embedding location by looking at the general parameters that formed the embedding location formula. Then, examine the time complexity of the watermark image extraction from the host image.

The DWT-Hungarian embedding equation described in section III contains three main factors that ensure the randomness of the embedding locations, increasing the robustness of the proposed method against JPEG (30) compression, cropping (50%), scaling, rotation and blurring attacks, and improve the quality compare to other related work. This process allows pattern-less and irregular embedding locations in host image, which increases the difficulty of predicting the embedded watermark locations. Finally, in the extraction process by using private key, the watermark can be extracted easily.

4. EXPERIMENTAL RESULTS

In this section, proposed method evaluated by using the Structural Similarity Index (SSIM) and the Peak Signal-to-Noise Ratio (PSNR) to measuring the quality after embedding watermark to the host image. For Robustness measurement use Normalized Cross-Correlation (NCC) after attack happened to the watermarked image.

The experiments conducted in this section will use “Lena” image as color host image with size of 512×512 . For the watermark image use “Peugeot logo” image with size of $32 \times$

32. JPEG (30) compression, cropping (50%), scaling, rotation, blurring has been used as watermark attacks.

The proposed scheme process for embedding as below:

1. For counter value to create sub host used 100.
2. The sub host size array is $SH = \{512 \times 512 \mid 412 \times 412 \mid 312 \times 312 \mid 212 \times 212 \mid 112 \times 112\}$
3. The ratio array value is $R = \{747 \mid 660 \mid 799 \mid 486 \mid 43\}$. Based on this record R_2 has been chosen. The private key is 50.
4. After resize SH_2 and watermark image to 512×512 size, embed watermark by DWT level2 into SH_2 area. The PSNR value is 40.7969 and the SSIM value is 0.9994.

Figure 8 shows the host image (Lena), watermark image (Peugeot logo) and the watermarked image after embedding.

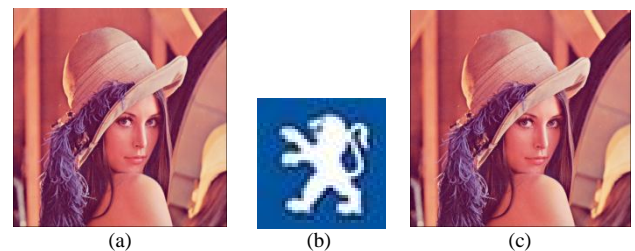


Figure 8: (a) Host image, (b) watermark, (c) watermarked image

Table 2 shows the quality of the proposed method compare to four other related works results (which used the same host image with the same size from the same CVG-UGR image database and the same watermark image with the same size)

after embedding watermark to host based on PSNR and SSIM. As it can be seen in Table 2, the proposed method has better quality compare to other related works results, which is 40.7969 for PSNR and 0.9994 for SSIM.

Table 2: Watermarked Image Quality Comparison

No.	References	Methods	PSNR	SSIM
1	Proposed Method	DWT, Hungarian Algorithm, Private key	40.7969	0.9994
2	[12]	Arnold Transform, Private key, MD5, Hessenberg Decomposition	36.3947	0.9371
3	[11]	Arnold Transform, Private key, MD5, LU Decomposition	39.4428	0.9816
4	[10]	Arnold Transform, Private key, Schur Decomposition	35.8031	0.9889
5	[9]	Arnold Transform, Private key, MD5, QR Decomposition	36.3521	0.9889

Figure 9 and Figure 10 shows the proposed scheme results compare to the other related methods. As expected, the two values (PSNR and ISSM) are steadily improving. The

Hungarian algorithm will have more ROI options to choose better location with less effect to image quality.

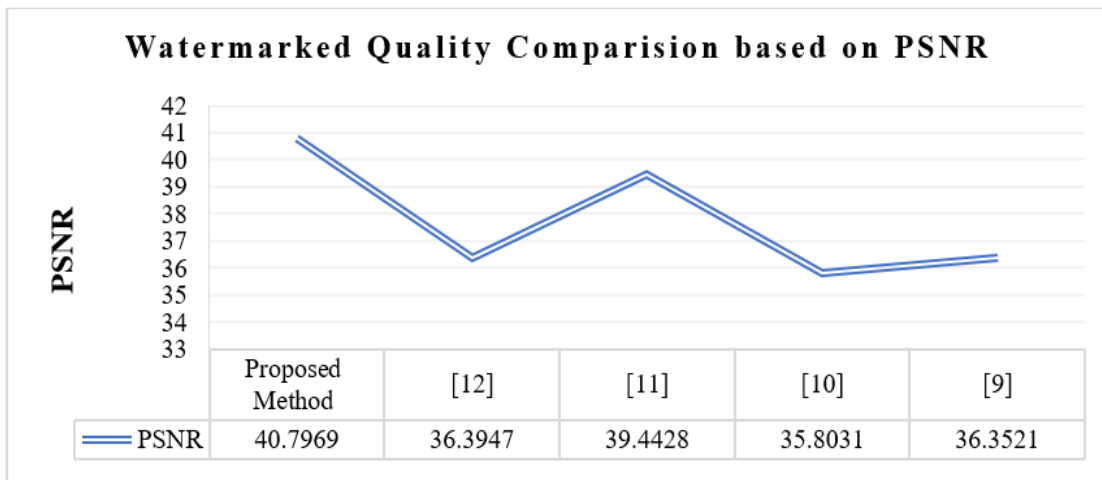


Figure 9: PSNR comparison results

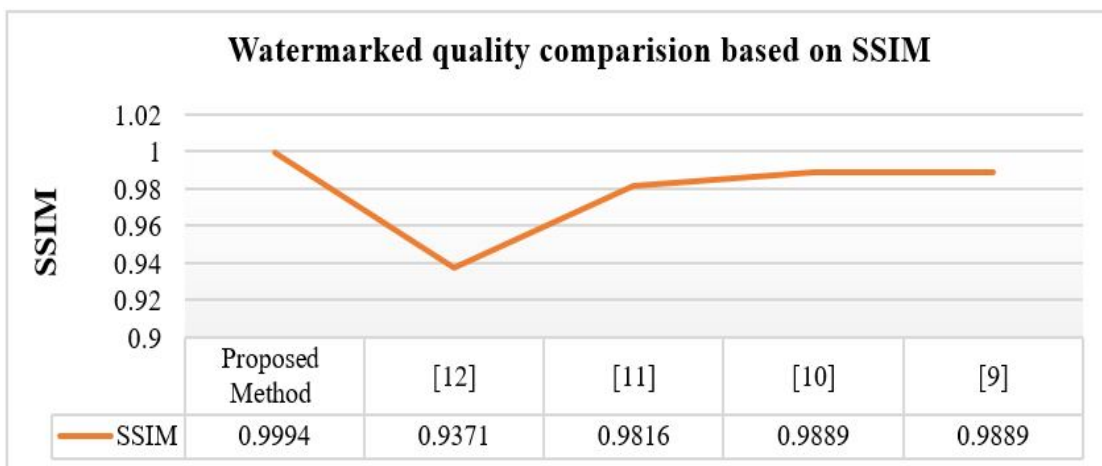


Figure 10: SSIM comparison results

The next step is to extract watermark image from watermarked images by using private key. The extraction steps are:


























1. Extract SH based on the private key 50.
2. Reverse DWT level two applied and watermark image extracted.

Based on the extracted watermark and original watermark image, the NCC value before attacked is one.

In this research the robustness has been improved for five attacks which are JPEG (30) compression, cropping (50%),

scaling, rotation, blurring and NCC value has been compared with other five related works' results (which used the same host image with the same size from the same CVG-UGR image database and the same watermark image with the same size). As it can be seen in Table 3 the proposed method robustness against these five watermarking attacks has been improved and NCC value for the proposed method is almost closed to ONE.

Table 3: NCC Result Comparison of Related Works with Proposed Method after Attacks

Host Image (Lena)						
Watermark Image (Peugeot logo)						
Attacks	[8]	[9]	[10]	[11]	[12]	Proposed method result
JPEG (30)						
	0.7530	0.9139	0.8528	0.9591	0.9486	0.973615
Cropping (50%)			-			
	0.5702	0.6264	-	0.8488	0.6319	0.894317
Scaling (4)						
	0.9823	0.9999	0.9932	0.9949	0.9980	0.999998
Rotation (5)				-	-	
	-	-	-	-	-	-
Blurring (1.0)				-	-	
	0.7839	0.7111	0.8790	-	-	0.906877

Based on Table 3, for JPEG attack the new proposed method results improved 0.02, cropping improved 0.04, and blurring improved 0.03 percent. The best results come from scaling in new methods.

Overall overview shows that proposed method has better watermark quality after attacks, especially in case of scaling and blurring attacks. Also, for rotation attack, the extracted watermark is more visible compare to other related works' results.

5. CONCLUSION AND FUTURE WORK

In this paper, a novel technique proposed to improve robustness and quality of watermarking method based on color image. For experimental result use the same host and watermark image ("Lena" as host image and "Peugeot logo" as watermark) which used by other five researchers from the same CVG-UGR image database. To evaluate the proposed method with other related works' results, PSNR and SSIM has

been used to check the quality result of watermarked image and NCC has been used to check the robustness after attacked. The result shows that the new proposed method has higher quality and stronger robustness compare to other related works.

For the future work, the proposed method can be extended to use SVD together with DWT to improve the robustness and test with many types of watermarking attacks. In addition, there is possibility to improve the way to find the better ROI by using fussy logic.

REFERENCES

[1] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *International Journal of Computational Intelligence Systems*, vol. 8, no. 2, pp. 364-380, 2015.

- [2] <https://doi.org/10.1080/18756891.2015.1001958>
D. Vaishnavi and T. Subashini, "**Robust and invisible image watermarking in RGB color space using SVD**," *procedia computer science*, vol. 46, pp. 1770-1777, 2015.
- [3] <https://doi.org/10.1016/j.procs.2015.02.130>
L. Laur, P. Rasti, M. Agoyi, and G. Anbarjafari, "**A robust color image watermarking scheme using entropy and QR decomposition**," *Radioengineering*, vol. 24, 2015.
- [4] <https://doi.org/10.13164/re.2015.1025>
Q. Su and B. Chen, "**Robust color image watermarking technique in the spatial domain**," *Soft Computing*, vol. 22, no. 1, pp. 91-106, 2018.
- [5] <https://doi.org/10.1007/s00500-017-2489-7>
H. Xu, G. Jiang, M. Yu, and T. Luo, "**A Color Image Watermarking Based on Tensor Analysis**," *IEEE Access*, vol. 6, pp. 51500-51514, 2018.
- [6] <https://doi.org/10.1109/ACCESS.2018.2866287>
T. Huynh-The *et al.*, "**Selective bit embedding scheme for robust blind color image watermarking**," *Information Sciences*, vol. 426, pp. 1-18, 2018.
- [7] <https://doi.org/10.1016/j.ins.2017.10.016>
J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "**iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning**," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1005-1016, 2017.
- [8] <https://doi.org/10.1109/TIFS.2016.2636090>
Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "**A blind double color image watermarking algorithm based on QR decomposition**," *Multimedia tools and applications*, vol. 72, no. 1, pp. 987-1009, 2014.
- [9] <https://doi.org/10.1007/s11042-013-1653-z>
Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "**Color image blind watermarking scheme based on QR decomposition**," *Signal Processing*, vol. 94, pp. 219-235, 2014.
- [10] <https://doi.org/10.1016/j.sigpro.2013.06.025>
Q. Su and B. Chen, "**An improved color image watermarking scheme based on Schur decomposition**," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24221-24249, 2016.
- [11] <https://doi.org/10.1007/s11042-016-4164-x>
Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "**A new algorithm of blind color image watermarking based on LU decomposition**," *Multidimensional Systems and Signal Processing*, pp. 1-20, 2017.
- [12] Q. Su and B. Chen, "**A novel blind color image watermarking using upper Hessenberg matrix**," *AEU-International Journal of Electronics and Communications*, vol. 78, pp. 64-71, 2017.
- [13] <https://doi.org/10.1016/j.aeue.2017.05.025>
Q. Su, Y. Niu, H. Zou, and X. Liu, "**A blind dual color images watermarking based on singular value decomposition**," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8455-8466, 2013.
- [14] <https://doi.org/10.1016/j.amc.2013.03.013>
Q. Su, Y. Niu, Q. Wang, and G. Sheng, "**A blind color image watermarking based on DC component in the spatial domain**," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 23, pp. 6255-6260, 2013.
- [15] <https://doi.org/10.1016/j.ijleo.2013.05.013>
Q. Su, Y. Niu, X. Liu, and T. Yao, "**A novel blind digital watermarking algorithm for embedding color image into color image**," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3254-3259, 2013.
- [16] <https://doi.org/10.1016/j.ijleo.2012.10.005>
J. Ouyang, G. Coatrieux, B. Chen, and H. Shu, "**Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping**," *Computers & Electrical Engineering*, vol. 46, pp. 419-432, 2015.
- [17] <https://doi.org/10.1016/j.compeleceng.2015.03.004>
A. Roy, A. K. Maiti, and K. Ghosh, "**A perception based color image adaptive watermarking scheme in YCbCr space**," in *Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on*, 2015, pp. 537-543: IEEE.
- [18] <https://doi.org/10.1109/SPIN.2015.7095399>
Q. Su, G. Wang, G. Lv, X. Zhang, G. Deng, and B. Chen, "**A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition**," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8781-8801, 2016.
- [19] <https://doi.org/10.1007/s11042-016-3522-z>
S. Bajracharya and R. Koju, "**An improved DWT-SVD based robust digital image watermarking for color image**," *International Journal Engineering and Manufacturing*, vol. 1, pp. 49-59, 2017.
- [20] <https://doi.org/10.5815/ijem.2017.01.05>
H. W. Kuhn, "**The Hungarian method for the assignment problem**," *Naval research logistics quarterly*, vol. 2, no. 1□2, pp. 83-97, 1955.
- [21] <https://doi.org/10.1002/nav.3800020109>
E. A. Alrashed, Suood Suood, "**Hungarian-Puzzled Text with Dynamic Quadratic Embedding Steganography**," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 2, pp. 799-809, 2017.
- [22] <https://doi.org/10.11591/ijece.v7i2.pp799-809>
A. Zear, A. K. Singh, and P. Kumar, "**A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine**," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4863-4882, 2018.
- [23] <https://doi.org/10.1007/s11042-016-3862-8>
E. Brannock, M. Weeks, and R. Harrison, "**Watermarking with wavelets: simplicity leads to robustness**," in *IEEE SoutheastCon 2008*, 2008, pp. 587-592: IEEE.
- <https://doi.org/10.1109/SECON.2008.4494361>

- [24] L. Ghouti, A. Bouridane, M. K. Ibrahim, and S. Boussakta, "**Digital image watermarking using balanced multiwavelets,**" *IEEE transactions on signal processing*, vol. 54, no. 4, pp. 1519-1536, 2006.
<https://doi.org/10.1109/TSP.2006.870624>
- [25] E. Dey, S. Majumder, and A. N. Mazumder, "**A new approach to color image watermarking based on joint DWT-SVD domain in YIQ color space,**" in *Electrical Information and Communication Technology (EICT), 2017 3rd International Conference on*, 2017, pp. 1-6: IEEE.
<https://doi.org/10.1109/EICT.2017.8275190>
- [26] H. Shojanazeri, W. A. W. Adnan, and S. M. S. Ahmad, "**Video watermarking techniques for copyright protection and content authentication,**" *International Journal of Computer Information Systems Industrial Management Applications*, vol. 5, no. 1, pp. 652-660, 2013.