A Novel Zero-Watermarking Based Scheme for Copyright Protection of Grayscale Images

MUHAMMAD FARHAN KHAN*, SYED MUHAMMAD GHAZANFAR MONIR**, AND IMRAN NASEEM*

RECEIVED ON 08.05.2018 ACCEPTED ON 17.08.2018

ABSTRACT

Zero-watermarking of digital images is a powerful method with respect to transparency in the watermarked image. However, robustness is still a challenging characteristic for researchers. The proposed method of zero-watermarking provides a novel solution for increasing robustness by obtaining resident features of grayscale image that are robust against common signal processing operations. The proposed solution is based on image scanning to produce NDD (NeighboringDistance Difference) profile. This scheme is used to extract image features for generating redundancy binary profile with the help of image scanning and identification of robust image areas for embedding a binary watermark. Redundant areas from binary profile show perceptually insignificant regions of grayscale image according to human visual system. Resident features from robust areas of image are collected to generate the zerowatermarking binary key image using reversible XOR operation. The binary key is used for extraction of binary watermark. Experimental results of the proposed method have been compared with the results of various zero-watermarking schemes as well as traditional watermarking methods and found much better at slightly higher computational cost. The comparison analysis for testing robustness has been carried out against image processing attacks like Gaussian filtering, block average filtering, motion blur filtering, image resizing, image rotation, image compression and cropping. For each attack maximum correlated watermark from the set of recovered watermarks is selected to evaluate the performance of proposed zero-watermarking scheme. It has been recorded that perfect matching is observed between original and extracted watermarks for a number of signal processing attacks.

Key Words: Copyright Protection, Image Scanning, Image Watermarking, Neighboring Distance Difference, Robust Feature Extraction.

1. INTRODUCTION

igital image watermarking is being used over two decades for applications such as copyright protection, document identification, authentication, colour or quality hiding, secret data hiding, etc. Conventionally a payload called digital watermark is inserted into the host image. This watermark may be inserted by direct manipulation of image pixels in spatial domain [1-4] or it may be inserted in transform-domain after applying a discrete transformation on original image [5-9].

Authors E-Mail: (farhanazeemi@hotmail.com, monir@jinnah.edu, imrannaseem@pafkiet.edu.pk, imran.naseem@uwa.edu.au)

* College of Engineering, PAF Karachi Institute of Economics and Technology, Karachi, Pakistan.

** Department of Electrical Engineering, Mohammad Ali Jinnah University, Karachi, Pakistan.

This is an open access article published by Mehran University Research Journal of Engineering and Technology, Jamshoro under the CC by 4.0 International License. 627 Inserting the watermark into host image, faces contradictory requirements of transparency and robustness. On one hand, the inserted watermark needs to be as much transparent as possible to maintain the fidelity of the watermarked image. On the other hand, the inserted watermark needs to be robust against intentional and unintentional attacks on the watermarked image. While the former requirement constraints to have a low energy watermark, the latter needs the watermark to be strong, consequently having a high energy. The tradeoff required for having robustness and transparency simultaneously has remained a topic of interest for researchers since the inception of the idea of digital image watermarking.

Recently, an alternate scheme by the name of zerowatermarking has become popular [10-13]. Rather than embedding a watermark in the host image, zerowatermarking applies cryptography by encrypting host image features matrix with digital watermark to produce a watermarking key. This key image with its host image and watermark is then stored in the database of intellectual property for copyright protection. As no watermark is actually embedded into the host image, the watermarked image is the same host image. In other words, the watermarked image is completely transparent.

We present a novel technique based on image scanning and BRF (Binary Robust Feature) profile generation rather than the use of transformations. We exploit the properties of human visual system to use redundant areas for encryption and watermarking key generation. Experimental results of our scheme are more robust in comparison to the other methods. Rest of the paper comprises of the background and literature review in section II, details of proposed zero-watermarking scheme are given in section III, experimental results and discussions in section IV, finally the paper is concluded in section V.

2. BACKGROUND AND LITERATURE REVIEW

Digital image watermarking techniques are comprising of spatial and transform-domain techniques. More or less all spatial domain watermarking methods modify the contents of host image in bit planes such as modifying LSB (Least Significant Bit), quantization of intensities or color values. Modification of quantization indices in watermarks were embedded by using [14] pixels of the host image in the spatial domain. Characteristics of histograms and specific color planes of suitable color models are also used for efficient watermarking using spatial domain techniques [15-17]. Patchwork [18-19] is also an example of spatial domain watermarking. The objective of this method is to identify whether the watermark is present or not in the host image.

Compared to spatial-domain, transform-domain methods are more widely applied because of robustness. Spatial domain watermarking methods are easy and have smaller payload than frequency or transform domain methods but are more fragile against signal processing attacks and especially for media compression operations. Most popular frequency transformations are DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) and DWT (Discrete Wavelet Transform) which are used for digital image watermarking. DCT based approach is used to embed the contents of watermark in spectral component of host image. Some algorithms related to DCT with JND (Just Noticeable Difference) approach can be seen in [20-22]. DWT is another transformation way sort selected level of frequency components in the host image. In [23] a DWT-PCA (Principal Component Analysis) based nonblind color image digital watermarking scheme is proposed. In [24-25] the HVS (Human Visual System) is exploited using DWT and watermark strength is adjusted with the help of weighting function. DFT based watermarking is

another popular scheme because of its robustness against rotational signal processing attacks [9,26].

Zero-watermarking schemes are better than other watermarking schemes in the sense that we can achieve maximum transparency with robustness because no watermark is embedded but encrypted. In [11] a zerowatermarking scheme has been proposed where host image binary feature matrix is formed by using DWT with SVD (Singular Value Decomposition) of nonoverlapping blocks from LL sub-band of nth level DWT of host image. This scheme of zero-watermarking was further improved [27] by using BN (Boost Normed) SVD approach for working in DWT domain. In [28] a blind watermarking algorithm based on zero-watermarking has been proposed using properties of visual cryptography, DFrFT (Discrete Fractional Fourier Transform) and SVD. The algorithm is further enhanced in [29] by the same author.

3. PROPOSED ZERO-WATERMARKING SCHEME

Proposed scheme of zero-watermarking is based on a novel image scanning method. The image scanning

method is shown with the help of blocks within dashed rectangle in Fig. 1. In this method the host image is processed in two branches. Upper branch of block diagram is used for extracting binary features of host image. The binary features show the texture behind the grayscale image and it named as RBM (Resident Binary Mark). While the lower branch of scanning algorithm develops the image profile according to robust spatial locations. The BRF is shown in block diagram. Finally robust resident features $k'_{u,v}$ are extracted by AND operation of RBM and BRF as illustrated in Fig. 1.

Zero-watermarking schemes are better than other watermark embedding schemes in the sense that we can achieve transparency with robustness because not a watermark is embedded but encrypted. Encryption of watermark with host image requires some robust features of host image so that at the time of decryption of watermark similar watermark can be identified from the disputed host image. Using non-robust features of the host image may result in a distorted watermark; therefore, the proposed zero-watermarking technique involves scanning of the host image for identifying robust spatial locations.



FIG. 1. ZERO-WATERMARKING KEY GENERATION

Mehran University Research Journal of Engineering & Technology, Volume 38, No. 3, July, 2019 [p-ISSN: 0254-7821, e-ISSN: 2413-7219] 629

3.1 Generation of Watermarking Binary Key

The proposed method of generation of watermarking binary key is a four-step procedure consisting of WTG (Watermark Tile Grid) generation, BRF profile generation, resident mark generation, and watermarking key generation. Block diagram of the proposed scheme is given in Fig. 1. To demonstrate steps of the proposed approach, we selected the images 4.2.03 (Baboon) and 4.2.04 (Lenna) from volume 3 of the USC-SIPI Image Database, University of Southern California, 1977 as host images. Size of the selected images after converting into grayscale is 512x512. The Star binary logo is used as a digital watermark Wwith dimensions 32x32 and is shown in Fig. 2(a).

Watermark Tile Grid Generation: WTG is a two dimensional array of binary watermarks and is used for embedding. Watermark is identified from each separate tile at the time of extraction and used for filtering noise so that a better quality watermark is reformed. Formation of WTG has two steps. First a binary mesh with white background and black equidistant horizontal and vertical lines is formed to make inner squares with same dimensions of watermark wm x wn. The size of nonoverlapping blocks is 1m x ln while the overall size of WTG is $u_{max} \ge v_{max}$, where $u_{max} = (n-2/lm, and v_{max} = (n-2/lm, and v_{max})$ In. This makes the size of WTG same as BRF profile. White squares are paved with watermark as tiles to form a two dimensional WTG $g_{\mu\nu}$ matrix as shown in Fig. 2(b). Right column and bottom row of the mesh tiles is filled with zeroes if smaller than wm x wn.

BRF Profile Generation: The host Image-I is scanned to find the redundant areas for embedding watermark. Pixels values $I_{i,j}$ are compared with their eight neighbour pixels $I_{ni,j}$ and maximum intensity distance is measured for worst case of redundancy. All image pixels are scanned one by

one leaving outer most rows and columns to form the redundancy profile. Here it should be kept in mind that higher intensity distance refers to lower redundancy. This collection forms NDD profile $d_{i,j}$ and may be considered as a greyscale image having size of (m-2) x (n-2) and expressed in Equation (1), where coordinates (i,j) ranges from second to second last row and column of host image respectively.

$$\mathbf{d}_{i,j} = \max_{1 \le n \le 8} \mathbf{D} \left(\mathbf{I}_{i,j}, \mathbf{I}_{n_{i,j}} \right) \tag{1}$$

where $I_{n_{i,j}}$ is nth neighbour of $I_{i,j}$ and D is the function for Euclidian distance between pixels $I_{i,j}$ and $I_{n_{i,j}}$.

Locations of $I_{i,j}$ and its neighbours $I_{n_{i,j}}$ are shown in Fig. 3(a-c). The NDD profile $d_{i,j}$ is divided into nonoverlapping blocks $p_{u,v}$ of size 3x3. Each block $p_{u,v}$ is used for embedding a single pixel of WTG. In case of binary watermark image, as we are considering here, each bit of



FIG. 2(a). BINARY WATERMARK (32X32)



WTG will be encrypted with every $p_{u,v}$ block. Maximum value from each $p_{u,v}$ block is taken to identify redundant blocks $p_{u,v}$. The size of $b_{u,v}$ is $u_{max} \times v_{mas}$ which is same as the WTG matrix. Finally, the BRF matrix is generated by comparing block maximum values to a threshold r. If the value of an element is less than r the logical equivalent is marked 1 or vice versa. This shows that lmxln block is suitable for embedding if its redundancy value is 1. The value of r is selected on the basis of the JND. The value of JND for human eye is 2.3 in Lab colour space [30]. The equivalent average value on grayscale is used in experiments. Robust profile $d_{i,j}$ and BRF are shown as images in Fig. 3(a-c). Mathematically BRF profile $p_{u,v}$ is expressed in Equation (2).

$$b_{u,v} = \begin{cases} 0 \text{ if } \max_{1 \le y \le \ln 1 \le x \le lm} \max_{u, v} (x, y) \ge r \\ 1 \text{ if } \max_{1 \le y \le \ln 1 \le x \le lm} \max_{u, v} (x, y) > r \end{cases}$$
(2)

Generation of Resident Binary Mark $k_{u,v}$: RBM is actually the binary image which can be extracted from the original host image without embedding any information. Accuracy of results depends on the matching level of extracted RBM from the tempered and original host image. RBM along with BRF and WTG is needed to develop the binary watermarking key. To develop the RBM image we extract MSBs from the host intensity image to compose a binary image. Most significant bit layer is chosen because it is the most robust against image processing attacks but this bit may also be changed because of a little addition or subtraction if lower bits of that pixel are at extremely minimum or maximum value. Therefore, we analyse 6th and 7th bits of pixels to decide whether the respective MSB should be considered or not. We use MSB (*Most Significant Bit*) of a pixel only if lower two bits show the medium state '01' or '10' otherwise the extracted MSB is marked '0'. This filtered binary image having the size (512x512) is named the resident image matrix $q_{i,j}$ and it is therefore, robust enough when extracted from the disputed image after tempering by an image processing attack.

Resident image $q_{i,j}$ is divided into non-overlapping blocks $q_{u,v}(x,y)$ with size lmxln leaving outer most rows and columns to make compatible with the blocks of BRF. Since each block will be used for encrypting an individual pixel of watermark therefore a single bit is extracted as resident bit $k_{v,u}$ from each block $q_{u,v}(x,y)$. $k_{u,v}$ is the resident binary matrix RBM and formulated by counting number of ones in blocks $q_{u,v}(x,y)$. If the count of ones is greater than half the number of bits in the block, then resident bit is marked one otherwise it is taken to be zero as calculated in Equation (3).



Mehran University Research Journal of Engineering & Technology, Volume 38, No. 3, July, 2019 [p-ISSN: 0254-7821, e-ISSN: 2413-7219] 631

$$b_{u,v} = \begin{cases} 0 \text{ if } \sum_{y=1}^{\ln} \sum_{x=1}^{\ln} q_{u,v}(x,y) \le \frac{\ln \times \ln}{2} \\ 1 \text{ if } \sum_{y=1}^{\ln} \sum_{x=1}^{\ln} q_{u,v}(x,y) > \frac{\ln \times \ln}{2} \end{cases}$$
(3)

where (u,v) ranges from (1,1) to (m-2)/lm, (n-2)/ln.

Black areas in BRF image are unsuitable for embedding therefore we donot want to use these places in RBM image for robust key generation. Logical AND operation is applied on RBM ($k_{u,v}$) and BRF ($b_{u,v}$) to filter out undesired locations. RBM and its filtered matrix $k'_{u,v}$ are shown in Fig. 4(a-b) and expressed in Equation (4).

$$k'_{u,v} = k_{u,v} \text{ and } b_{u,v}$$
 (4)

Watermarking Key Generation: The filtered RBM $k'_{u,v}$ is a binary image. It is robust against most of the intentional or unintentional image processing attacks i.e. it remains unchanged even extracted after intense attacks. Watermarking key can be generated by applying a reversible operation on the filtered RBM image. Exclusive OR is commonly used for reversible binary operations. So the $k'_{u,v}$ is XORed with WTG to get the watermarking key $y_{u,v}$ as formulated in Equation (5).



FIG. 4(a). RBMk_{u,v} (170x170)

$$\mathbf{y}_{u,v} = \mathbf{k'}_{u,v} \oplus \mathbf{g}_{u,v} \tag{5}$$

At the time of extraction, the watermarking key is again XORed with the extracted filtered RBM image to recover the WTG image.

3.2 Identification of Disputed Image Using Registered Binary Key

The disputed image might be attacked by several image processing operations performed intentionally or unintentionally. Disputed image is first scanned in the same way as given in Fig. 1 to produce robust resident features $k'_{u,v}$ as illustrated in Fig. 5 by a single block of image scanning.



FIG. 5. ZERO-WATERMARK IDENTIFICATION SCHEME



FIG. 4(b). FILTERED RBMk'_{uv} (170x170)

Since the registered key is available at the time of identification therefore robust resident matrix $k'_{u,v}$ is operated with registered binary key using XOR to recover WTG array. Watermark tiles from recovered WTG might be in distorted state because of image processing attacks. Therefore, it is further processed to extract out the watermark tile having maximum correlation with original watermark from WTG array as shown in Fig. 6.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

Extensive experiments have been performed to verify the robustness of watermarking scheme. Standard colour images volume 3 of the USC-SIPI Image Database are first converted into grayscale and scanned for developing watermarking keys. Grayscale host images are subjected to different kinds of image processing attacks to analyse the robustness. These attacked images are tested for their PSNR (Peak Signal to Noise Ratio) and used to recover the watermark with the help of watermarking key. NC (Normalized Correlation) is an efficient tool for similarity measurement of binary images. Therefore, NC values are also measured for quality assessment of identified watermark. We used the relation given in Equation (6) to find NC values for pairs of recovered and original watermarks.

$$NC = \frac{1}{Wm \times Wn} \sum_{j=1}^{Wn} \sum_{i=1}^{Wm} \overline{W_{i,j} \oplus W_{i,j}}$$
(6)

where $W_{i,j}$ and $W'_{I,j}$ are original and recovered watermarks.

Recovered Watermark Quality Analysis against Some Common Attacks and Comparison with Previous Work: SSIM (Structural Similarity) and PSNR approaches are most widely used quantitative measures to assess image fidelity. SSIM is more effective for similarity of two different images while PSNR is an effective way to find the noise contents [31].



Mehran University Research Journal of Engineering & Technology, Volume 38, No. 3, July, 2019 [p-ISSN: 0254-7821, e-ISSN: 2413-7219] 633

Addition of Noise and Recovered Watermarks: Following are some noisy versions of standard images Lenna and Baboon. A number of image processing operations are performed as attacks. Gaussian noise with zero-mean and variance from 0.01-0.15, motion blurring from 9-30 pixels with 45p, block averaging 3x3-13x13, image resizing 128x128-1024x1024, image rotation 1-5p, JPEG compression with quality factor 10-100%, image horizontal and vertical cropping 10-80% are performed on standard grayscale referred in section III A. Contents and type of noise with PSNR are specified in captions of Fig. 7(a-p).



FIG. 7(a) GAUSSIAN PSNR 10.2 (b) GAUSSIAN PSNR 10.2 (c) MOTION PSNR 23.0 (d) MOTION PSNR 19.4 (e) AVERAGING PSNR 24.4 (f) AVERAGING PSNR 19.7 (g) RESIZE 128X128 PSNR 28.8 (h) RESIZE 128X128 PSNR 21.1 (i) ROTATE 5° PSNR 14.7 (j) ROTATE 5° PSNR 14.7 (k) JPEG10% PSNR 30.4 (l) JPEG10% PSNR 23.4 (m) HORIZONTAL CROP 80% PSNR 6.6 (n) HORIZONTAL CROP 80% PSNR 6.2 (o) VERTICAL CROP 80% PSNR 6.5 (p) VERTICAL CROP 80% PSNR 6.4

Proposed identification algorithm is applied on noisy images to recover the watermark using their respective zero-watermarking keys. Maximum correlated recovered watermarks from images given in Fig. 7(a-p) are illustrated in Fig. 8(a-p) respectively. Recovered watermarks are further analysed by using NC for robustness comparison of the proposed algorithm to previous methods presented in [28-29,31-33]. NC results of previous schemes are taken from Rani [29] and compiled in Tables1-2 with proposed solution for comparison of robustness.



FIG. 8. RECOVERED BINARY WATERMARKS FROM ATTACKED IMAGES

PSNR	NC						
	Chen [33]	Hsu [31]	Wang [32]	Rawat [28]	Rani [29]	Proposed	
						Maximum NC	
10.4	0.89	0.78	0.90	0.89	0.90	1.00	
11.5	0.90	0.79	0.91	0.90	0.91	1.00	
13.9	0.90	0.80	0.93	0.93	0.94	1.00	
14.8	0.91	0.81	0.93	0.93	0.95	1.00	
15.9	0.92	0.82	0.95	0.94	0.95	1.00	
17.4	0.94	0.84	0.96	0.95	0.96	1.00	
20.2	0.94	0.86	0.96	0.96	0.97	1.00	

TABLE 1. PSNR VS NC FOR GAUSSIAN ATTACKED LENNA IMAGES

TABLE 2. PSNR VS NC FOR JPEG COMPRESSED LENNA IMAGES

PSNR	NC						
	Chen [33]	Hsu [31]	Wang [32]	Rawat [28]	Rani [29]	Proposed	
						Maximum NC	
30.2	0.974	0.973	0.977	0.977	0.977	1.000	
32.1	0.985	0.984	0.989	0.989	0.990	1.000	
33.3	0.987	0.990	0.993	0.991	0.991	1.000	
33.9	0.990	0.995	0.994	0.993	0.994	1.000	
34.3	0.991	0.996	0.995	0.995	0.995	1.000	
34.7	0.994	0.996	0.995	0.997	0.996	1.000	
35.3	0.995	0.998	0.997	0.998	0.997	1.000	

Results can be analysed with the help of data tables and graphs shown in Fig. 9(a-b) against two different kinds of signal processing attacks.

Analysis of Robustness against Redundancy Threshold: Elements of NDD profile $d_{i,j}$ are divided into nonoverlapping blocks as expressed in Equation (2). Maximum value from each block is compared with the redundancy threshold to identify whether the block is redundant or not for embedding. The redundancy threshold is selected on the basis of JND. The threshold 'r' is also used to set the robustness of scheme. There is



Mehran University Research Journal of Engineering & Technology, Volume 38, No. 3, July, 2019 [p-ISSN: 0254-7821, e-ISSN: 2413-7219] 636

an inverse relation between redundancy 'r' and robustness. Lower values of 'r' cause decrement in discrimination capability or the true positive rate. Watermark tiles recovered from JPEG compressed Lenna image, with quality factor of 10%, are numbered from 1-25 and NC for each tile with original watermark is evaluated and shown in Table 3 for some suitable values of 'r'. Mean and maximum values are also evaluated at the end of Table 3. It is evident from results that the independent variable 'r' is the main parameter through which 100% recovery is optimized.

TABLE 3. RECOVERED WATERMARKS FROM JPEG LENNA IMAGE AND THEIR NC VALUES FOR SOME SUITABLE
VALUS OF 'R'

	NC					
Recovered Watermark Tile	r = 10	r = 20	r = 30	r = 40		
1	0.768	0.724	0.724	0.724		
2	1.000	1.000	1.000	1.000		
3	0.969	0.854	0.734	0.711		
4	0.953	0.951	0.951	0.950		
5	0.953	0.933	0.911	0.892		
6	0.830	0.801	0.801	0.801		
7	1.000	0.998	0.974	0.938		
8	0.938	0.606	0.459	0.425		
9	0.674	0.508	0.440	0.396		
10	0.888	0.854	0.846	0.840		
11	0.818	0.775	0.775	0.775		
12	1.000	0.994	0.985	0.979		
13	0.943	0.803	0.756	0.740		
14	0.854	0.729	0.696	0.684		
15	0.833	0.800	0.793	0.793		
16	0.812	0.771	0.771	0.771		
17	1.000	0.999	0.991	0.987		
18	0.966	0.935	0.934	0.934		
19	0.995	0.959	0.930	0.907		
20	0.666	0.635	0.616	0.609		
21	0.822	0.718	0.715	0.711		
22	1.000	1.000	1.000	1.000		
23	0.998	0.998	0.998	0.998		
24	0.514	0.486	0.484	0.484		
25	0.894	0.847	0.801	0.776		
Mean NC	0.883	0.827	0.803	0.793		
Maximum NC	1.000	1.000	1.000	1.000		

Tang et. al. [34] have also developed such algorithm and evaluated statistical results. They have also achieved 100% similarities. Results of Tang and proposed scheme are compared in Table 4 against Gaussian noise and JPEG compression.

The proposed scheme embeds an array of 5x5 watermark tiles rather a single watermark. Therefore, the recovered binary image has 25 watermarks with noise contents. Fig. 6 shows the extracted noisy watermarks with tile numbers from JPEG compressed Lenna image with quality factor of 10%.

5. CONCLUSIONS

The presented watermarking scheme is based on the idea of image scanning to explore the suitable spatial locations according to human visual system for extracting robust features of image. A novel technique NDD profile generation has been introduced for developing the binary robust image. The BRF profile is generated by applying JND threshold on NDD profile. This provides precisely the areas suitable for zero-watermarking according to HVS. Robust image features are extracted from these selected areas $k_{u,v}$. Two dimensional array of binary watermark WTG is used for encryption instead of a single watermark image. Finally, a robust zero-watermarking key is generated. Using this key, the array of watermarks is extracted and maximum matched binary watermark can easily be filtered from the array with the help of highest value of NC. That is why the NC values of extracted watermarks are so ideal in our proposed scheme.

ACKNOWLEDGEMENT

The authors would like to appreciate their respective institutes for facilitating this research.

REFERENCES

- Tirkel, A., Rankin, G.A., van Schyndel, R.J., Ho, W., Mee, N., and Osborne, C., "Electronic Watermark", Digital Image Computing, Technology and Applications, pp. 666–672, 1993.
- [2] Cox, I.J., Kilian, J., Leighton, T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Images, Audio and Video", Proceedings of 3rd IEEE International Conference on Image Processing, Volume 3, pp. 243-246, 1996.
- [3] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Volume 6, No. 12, pp. 1673-1687, 1997.
- [4] Watson, A.B., "DCT Quantization Matrices Visually Optimized for Individual Images", IS&T/SPIE's Symposium on Electronic Imaging: Science and Technology, Volume 1913, pp. 15, 1993.
- [5] Patra, J.C., Phua, J.E., and Bornand, C., "A Novel DCT Domain CRT-Based Watermarking Scheme for Image Authentication Surviving JPEG Compression", Digital Signal Processing, Volume 20, No. 6, pp. 1597-1611, 2010.

Operation	Similarity from F	roposed Scheme	Similarity from Tang Scheme [34]		
Operation	Mean	Max.	Mean	Max.	
3x3 Gaussian low-pass filtering	0.827	1.000	0.9741	1.000	
JPEG Compression	0.883	1.000	0.940	0.998	

TABLE 4. RECOVERED WATERMARKS FROM JPEG LENNA IMAGE AND THEIR NC VALUES VS REDUNDENCY 'R'

- [6] Akter, A., Nur, E.T., and Ullah, M.A., "Digital Image Watermarking Based on DWT-DCT: Evaluate for a New Embedding Algorithm", International Conference on Informatics, Electronics & Vision, pp. 1-6, 2014.
- [7] Dubolia, R., Singh, R., Bhadoria, S.S., and Gupta, R., "Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR", International Conference on Communication Systems and Network Technologies, pp. 593-596, 2011.
- [8] Ali, M., Ahn, C.W., and Pant, M., "A Robust Image Watermarking Technique Using SVD and Differential Evolution in DCT Domain", Optik - International Journal for Light and Electron Optics, Volume 125, No. 1, pp. 428-434, 2014.
- [9] Hong-Ying, Y., Xiang-Yang, W., Pei, W., and Pan-Pan, N., "Geometrically Resilient Digital Watermarking Scheme Based on Radial Harmonic Fourier Moments Magnitude", AEU - International Journal of Electronics and Communications, Volume 69, No. 1, pp. 389-399, 2015.
- [10] Cao, H., Xiang, H., Li, X., Liu, M., Yi, S., and Wei, F., "A Zero-Watermarking Algorithm Based on DWT and Chaotic Modulation", Defense and Security Symposium, Volume 6247, pp. 9, 2006.
- [11] Yaxun, Z., and Wei, J., "A Novel Image Zero-Watermarking Scheme Based on DWT-SVD", International Conference on Multimedia Technology, pp. 2873-2876, 2011.
- [12] Tsai, H.-H., Lai, Y.-S., and Lo, S.-C., "A Zero-Watermark Scheme with Geometrical Invariants Using SVM and PSO Against Geometrical Attacks for Image Protection", Journal of Systems and Software, Volume 86, No. 2, pp. 335-348, 2013.
- [13] Jalil, Z., Mirza, A.M., and Iqbal, T., "A Zero-Watermarking Algorithm for Text Documents Based on Structural Components", International Conference on Information and Emerging Technologies, pp. 1-5, 2010.

- [14] Chou, C.-H., and Wu, T.-L., "Embedding Color Watermarks in Color Images", EURASIP Journal on Advances in Signal Processing, No. 1, pp. 548941, 2003.
- [15] Lin, C.-H., Chan, D.-Y., Su, H., and Hsieh, W.-S., "Histogram-Oriented Watermarking Algorithm: Colour Image Watermarking Scheme Robust Against Geometric Attacks and Signal Processing", IEE Proceedings - Vision, Image and Signal Processing, Volume 153, No. 4, pp. 483-492, 2006.
- [16] Mohanty, S.P., Sheth, R., Pinto, A., and Chandy, M., "CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images", IEEE International Symposium on Consumer Electronics, pp. 1-6, 2007.
- [17] Nasir, I., Weng, Y., and Jiang, J., "A New Robust Watermarking Scheme for Color Image in Spatial Domain",3rdInternational IEEE Conference on Signal-Image Technologies and Internet-Based System, pp. 942-947, 2007.
- [18] In-Kwon, Y., and Hyoung Joong, K., "Modified Patchwork Algorithm: ANovel Audio Watermarking Scheme", IEEE Transactions on Speech and Audio Processing, Volume 11, No. 4, pp. 381-386, 2003.
- [19] Cvejic, N., and Seppanen, T., "Robust Audio Watermarking in Wavelet Domain Using Frequency Hopping and Patchwork Method", Proceedings of 3rd International Symposium on Image and Signal Processing and Analysis, Volume 1, pp. 251-255, 2003.
- [20] Piva, A., Bartolinin, F., Cappellini, V., and Barni, M., "Exploiting the Cross-Correlation of RGB-Channels for Robust Watermarking of Color Images", International Conference on Image Processing, Volume 1, pp. 306-310, 1999.
- [21] Ahmidi, N., and Safabakhsh, R., "A Novel DCT-Based Approach for Secure Color Image Watermarking", Proceedings of International Conference on Information Technology: Coding and Computing, Volume 2, pp. 709-713, 2004.

A Novel Zero-Watermarking Based Scheme for Copyright Protection of Grayscale Images

- [22] Chun-Hsien, C., and Yun-Chin, L., "A Perceptually Tuned Subband Image Coder Based on the Measure of Just-Noticeable-Distortion Profile", IEEE Transactions on Circuits and Systems for Video Technology, Volume 5, No. 6, pp. 467-476, 1995.
- [23] Kumar, A., and Gupta, M., "Semi Visible Watermarking Scheme Based on DWT and PCA", International Conference on Green Computing and Internet of Things, pp. 986-990, 2015.
- [24] Podilchuk, C.I., and Wenjun, Z., "Image-Adaptive Watermarking Using Visual Models", IEEE Journal on Selected Areas in Communications, Volume 16, No. 4, pp. 525-539, 1998.
- [25] Kaewamnerd, N., and Rao, K.R., "Wavelet Based Image Adaptive Watermarking Scheme", Electronics Letters, Volume 36, No. 4, pp. 312-313, 2000.
- [26] Licks, V., and Hordan, R., "On Digital Image Watermarking Robust to Geometric Transformations", Proceedings of International Conference on Image Processing, Volume 3, pp. 690-693, 2000.
- [27] Rao, Y.R., and Nagabhooshanam, E., "A Novel Image Zero-Watermarking Scheme Based on DWT-BN-SVD", International Conference on Information Communication and Embedded Systems, pp. 1-6, 2014.

- [28] Rawat, S., and Raman, B., "A Bwatermarking Algorithm Based on Fractional Fourier Transform and Visual Cryptography", Signal Processing, Volume 92, No. 6, pp. 1480-1491, 2012.
- [29] Rani, A., and Raman, B., "An Image Copyright Protection Scheme by Encrypting Secret Data with the Host Image", Multimedia Tools and Applications, Volume 75, No. 2, pp. 1027-1042, 2016.
- [30] Liu, K.-C., and Chou, C.-H., "Robust and Transparent Watermarking Scheme for Colour Images", IET Image Processing, Volume 3, No. 4, pp. 228-242, 2009.
- [31] Hsu, C.-S., and Hou, Y.-C., "Copyright Protection Scheme for Digital Images Using Visual Cryptography and Sampling Methods", Optical-Engineering, Volume 44, No. 7, pp. 077003, 2005.
- [32] Shih-Hao, W., and Yuan-Pei, L., "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions on Image Processing, Volume 13, No. 2, pp. 154-165, 2004.
- [33] Tzung-Her, C., Horng, G., and Wei-Bin, L., "A Publicly Verifiable Copyright-Proving Scheme Resistant to Malicious Attacks", IEEE Transactions on Industrial Electronics, Volume 52, No. 1, pp. 327-334, 2005.
- [34] Tang, Z., Huang, L., Zhang, X., and Lao, H., "Robust Image Hashing Based on Color Vector Angle and Canny Operator", AEU - International Journal of Electronics and Communications, Volume 70, No. 6, pp. 833-841, 2016.