2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) | 978-1-6654-6390-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/IISA56318.2022.9904378

A Repetitive Watermarking Scheme for Digital Images based on Self-Inverting Permutations

Maria Chroni
Dept. of Computer Science & Engineering
University of Ioannina
Ioannina, Greece
mchroni@uoi.gr

Stavros D. Nikolopoulos
Dept. of Computer Science & Engineering
University of Ioannina
Ioannina, Greece
stavros@cs.uoi.gr

Iosif Polenakis
Dept. of Computer Science & Engineering
University of Ioannina
Ioannina, Greece
ipolenak@cs.uoi.gr

Vasileios Vouronikos
Dept. of Computer Science & Engineering
University of Ioannina
Ioannina, Greece
v.vouronikos@uoi.gr

***Abstract*—In this work we present a novel watermarking scheme based on the repetitive application of watermarks inside a digital image. Our approach extends the technique proposed initially in [1] and [2] by implementing the corresponding approach repetitively over the wider area of the digital image and embedding the whole watermark in the corresponding cells instead of parts of it. The approach proposed in this work focuses mainly on securing the watermarked image against crop attacks and compression attacks that constitute the most important attacks through the attack vectors. Our approach provides a significant improvement over the computational cost required for the embed procedure of the watermark inside a digital image, achieving an adequately imperceptible and robust watermarking technique. The experimental results exhibited through the evaluation of our proposed model prove its potentials against these types of attacks and ensure that the embedded information will be successful extracted from the watermarked image after the deployment of such attacks.**

***Index Terms*—Image watermarking, Security, Digital Rights, Graph Theory**

I. Introduction

Digital watermarking is a type of information concealment that is used to secure a digital object. A watermark is a unique identifier that is put in a digital object when it is watermarked. The watermark indicates a single owner and legal holder of the digital thing in question since it is unique. Even if the digital object has been modified by a hostile attack, a watermarking approach is efficient if the watermark is efficiently embedded in the digital object and successfully removed. Since the amount of data (pictures) we send every day has expanded, digital image watermarking has become increasingly crucial. Nowadays, a digital image has evolved into a commercial product, and protecting it is critical. A characteristic example is medical digital images used for e-health, where the usage of watermarks on medical images is critical [3]. Watermarking schemes that are more secure have been developed in response to the necessity to keep this data secure and the significant growth in the speed of computing systems.

A. Related Work

A watermarking technique for medical images in e-health care systems is described in [3]. The vector picture is a medical image, and the watermark is a copy of the patient's health card. In oorder to embed the watermark in an image, the image and the watermark are first modified using the Discrete Wavelet Transform (DWT), and the individual areas of the DWT transformation are then changed to the RGB model. The SV values of the watermark are then incorporated into the SV values of the vector picture using the Singular Value Decomposition (SVD) transform. Each patient's health card is therefore integrated into his medical data. Recently, Sinhal *et al.* in [4] proposed a blind and robust scheme for color image watermarking, utilizing the YCbCr color space, the Integer Wavelet Transform (IWT), and the Discrete Cosine Transform (DCT). For picking the blocks to embed the watermark bits, they used a randomization approach based on Mersenne Twister random generator, while an Artificial Neural Network (ANN) framework developed in order to lower the computational complexity of the embedding process in order to provide a faster response.

Two watermarking approaches for medical images proposed by Fares *et al.* in [5] preserving the confidentiality of personal data by safeguarding patient information through the use of a hash contained in the image. These approaches ensure the integrity of the hidden data. A blind spatial-domain and frequency-domain image watermarking scheme is proposed by Yuan *et al.*, in [6] that combines DCT and Discrete Hartley Transform (DHT), utilizing unique properties of the DC components of DCT and DHT. Malayil and Vedhanayagam in [7] proposed a reversible watermarking system that can be used for both Electronic Patient record (EPR) transmission and medical image authentication. Authors of [7] introduce a novel image scaling up procedure to embed the watermark (authentication code and EPR) into the medical image, while a set of rules is defined to embed authentication code and EPR data in the new scaled-up image by copying neighbor pixels as the missing pixel intensity values. A robust and imperceptible watermarking scheme is presented in [8] by Gong *et al.*, combining Canny edge detection, contourlet transform, and

singular value decomposition to improve the invisibility and robustness of the watermarking algorithm. In [9] Meliimi *et al.*, proposed a fast watermarking scheme based on the Lifting Wavelet Transform (LWT) and Deep Neural Network (DNN). Wavelet transforms are used in watermark embedding to maintain a high level of imperceptibility and robustness. The best balance between robustness and imperceptibility is found by experimenting with different frequency bands.

Moad *et al.*, proposed a watermarking approach for patient identification and watermark integrity verification in [10], where the watermark is divided into two parts: the first comprises the patient's information fingerprint, and the second contains the patient's encrypted image. In [11] Yan *et al.*, proposed a multi-watermarking scheme for medical images based on quantum random walk and the brain storm optimization technique. To conceal private hospital and patient information, a logo image which has been used to check medical image integrity, was placed in regions of interest, whereas text data was embedded in regions of non-interest. This method increases medical picture verification accuracy and helps to assure authenticity. Recently, Faheem *et al.*, in [12] proposed a watermarking scheme in which an original image is broken into 16×16 blocks and a gradient is used to determine the magnitude and direction of each block. The gradient magnitude represents image changes, whereas the gradient angle represents change direction, and the middle coefficient is utilized for embedding. The aforementioned approach has a high level of robustness and imperceptibility.

B. Motivation and Contribution

One of the main concerns over the investigation of robustness of the watermarking techniques against attacks, is the case where segments of a digital image have been cropped and their authority can not be claimed by their original author. The main reason that such cases may occur results from the fact that in these segments of the digital image the hidden information may not be adequate to prove the identity of the author. In particular, the most common type of geometrical attack deployed by digital image processing tools can crop specific segments of a digital image such that no hidden information can be successfully extracted. Regarding the graph-based approach proposed in [1] and [2], it is proposed a quite robust watermarking technique that even being quite resilient against most of the attacks, still it can not perform adequately (i.e., to extract successfully the corresponding hidden information) when applied in a cropped segment of the watermarked image.

In this work, we extend the technique proposed initially in [1] and [2] by implementing the corresponding approach repetitively over the wider area of the digital image and embedding the whole watermark in the corresponding cells instead of parts of it. In particular, we utilize the initial algorithm proposed in [2] to locate the cells of the image that the information will be placed utilizing the 2DM representation of the Self-inverting Permutation (SiP) that encodes an integer w, while we use the same procedure repetitively in order to embed the whole watermark inside these cells.

II. The Model

In this section we present the proposed repetitive watermarking techniques to embed and extract integers encoded as self-inverting permutations into digital images.

A. Encoding and Decoding Information

To embed an integer number in an image, we must first convert it into a Self-inverting Permutation (SiP), which contains the watermark, and then convert it back to an integer during the extraction procedure to ensure we get back the information we originally embedded, following the corresponding methodologies as described in [1]. As described in [1], we use the Discrete Fourier Transform (DFT) to embed the watermark in the image using the amplitude of the frequencies. The watermark is inserted at certain sections of the 2DM representation, namely at points indicated with a specific symbol in the proposed approach of self-inverting permutations (see, Figures 1 and 2). The input image is transformed in the frequency domain using the 2D DFT. The DFT amplitude matrices are marked using two ellipsoidal annuli, namely the 'Blue' and 'Red', respectively. During the extraction we reverse the procedure by discovering the marked cells and construct the permutation π^*.

The proposed repetitive watermarking scheme ensures that derived (i.e., watermarked) image maximizes its fidelity against the initial image, while the hidden information is as robust as possible against potential attacks, w.r.t. the resilience of the embed and extract procedures. In terms of the fidelity, the proposed repetitive watermarking scheme is evaluated using the *Peak to Signal Noise Ratio* (PSNR) and *Structured Similarity Index Metric* (SSIM), which we will discuss later. On the other hand, we evaluate the robustness of the proposed watermarking scheme in order to prove that the hidden information is well preserved and the corresponding technique is resilient against various attacks (e.g., compression, geometric). The proposed repetitive watermarking scheme ensures that the hidden information can be extracted even through the direct extraction of at least one of the embedded watermarks, or by its reconstruction. The robustness of the proposed scheme against attacks is proven by the fact that in a any case, at least one, or all, the embedded watermarks can be directly extracted, or extracted and then be reconstructed, deriving finally the information embedded by the author of the image. The proposed repetitive watermarking scheme deploys the implementation of the corresponding embedding and extraction procedures described next by presenting the underlying fundamental components of each one.

B. Repetitive Embed of Watermarks into Digital Images

The implementation of our proposed repetitive watermarking scheme includes the sequential utilization of the watermarking procedure described in [2]. In particular, we deploy the 2DM representation of SiP, which encodes an integer w and is used to locate specific cells of an image I in order to sequentially embed the watermarks into these areas of the image as follows:

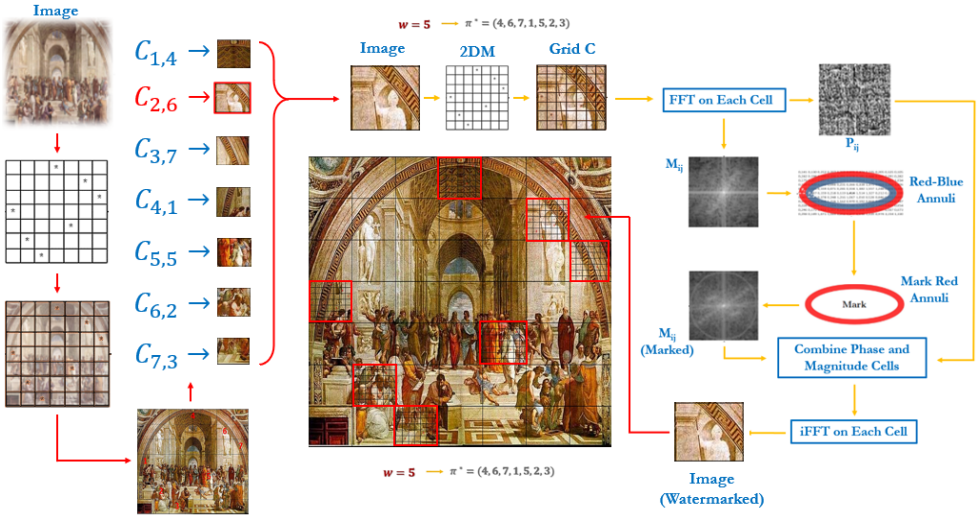


Fig. 1: Embed procedure architecture.

Data: Image I, Integer Number w to be Embedded in the Image I
Result: Watermarked Image I_w
Construct 2DM representations of $Sip(w)$;
for *marked cell in the 2DM representations* **do**
  Select the corresponding cells in I;
  for *cell selected from I, let* $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$ **do**
    Construct 2DM representations of $Sip(w)$;
    for *marked cell in the 2DM representation* **do**
      select the corresponding cells in $C_{i,\pi^*(i)}$;
      for $C'_{i,j} \in C_{i,\pi^*(i)}$ **do**
        Compute the FFT on this cell;
        Extract the corresponding *magnitude* M_{ij} and *Phase* P_{ij} matrices ;
        Place the Red-Blue Annuli on M_{ij} ;
        if $C'_{i,j}$ *corresponds to a cell marked in the 2DM representation* **then**
          Mark the Red-Annuli of M_{ij};
        end
        Combine M_{ij} with P_{ij};
        Compute the iFFT on $C'_{i,j}$;
      end
    end
  end
end

Algorithm 1: Embed Algorithm utilizing the embed approach proposed in [2].

1) we select an integer w and utilize the 2DM representations of the SiP that encodes it, to locate the corresponding cells of the image, let $C_{i,j}$.
2) then, repetitively, for each cell $C_{i,j}$ we utilize again the same integer w and by the 2DM representations of the SiP that encodes it we select the cells $C'_{i,j}$ inside the boundaries of $C_{i,j}$ in order to mark them and embed inside $C_{i,j}$ the entire watermark.

In Algorithm 1, we present step-by-step the procedure of embedding repetitively a watermark into an image utilizing the proposed approach. The embedding procedure utilizes the 2DM representation of the SiP, in order to determine the cells of the image that would contain the hidden information, i.e. the entire watermarks. As we can observe from the illustrative example presented in Figure 1, the 2DM representation of the SiP, which encodes the integer w that we want to embed into the image I, defines the cells $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$. Then, applying the repetitive watermarking approach, as described from the proposed watermarking scheme, for each one of these $C_{i,\pi^*(i)}$ cells, we repeat the procedure by exploiting again the 2DM representation of the SiP, which encodes the integer w that we want to embed into the cell $C_{i,\pi^*(i)}$, to locate the corresponding cells $C'_{1,\pi^*(1)}, C'_{2,\pi^*(2)}, \dots C'_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$ inside the boundaries of an external cell, let $C_{i,j}$. Finally, following the procedure described in Section II-A the FFT process is applied for each cell $C'_{1,\pi^*(1)}, C'_{2,\pi^*(2)}, \dots C'_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$, each cell of each region, in order to compute the amplitude matrices that will be used to indicate the amplitudes of the selected region. The latest step is repeated over the cells inside the boundaries of each cell $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$. Finally, the image is reconstructed to its watermarked state using the inverse Fast Fourier Transformation technique.

C. Repetitive Extraction of Watermarks from Digital Images

Similarly to the ebbed procedure presented above, we deploy the 2DM representation of the SiP that encodes the integer w that is embedded in the image I to locate the specific cells of image I that contain the entire watermarks in order to sequentially extract the watermarks from these areas of the image as follows:

1) we utilize the 2DM representations of the SiP that encodes the integer w we previously embedded in the cells of I through the corresponding procedure, to locate the cells of the image, let $C_{i,j}$.

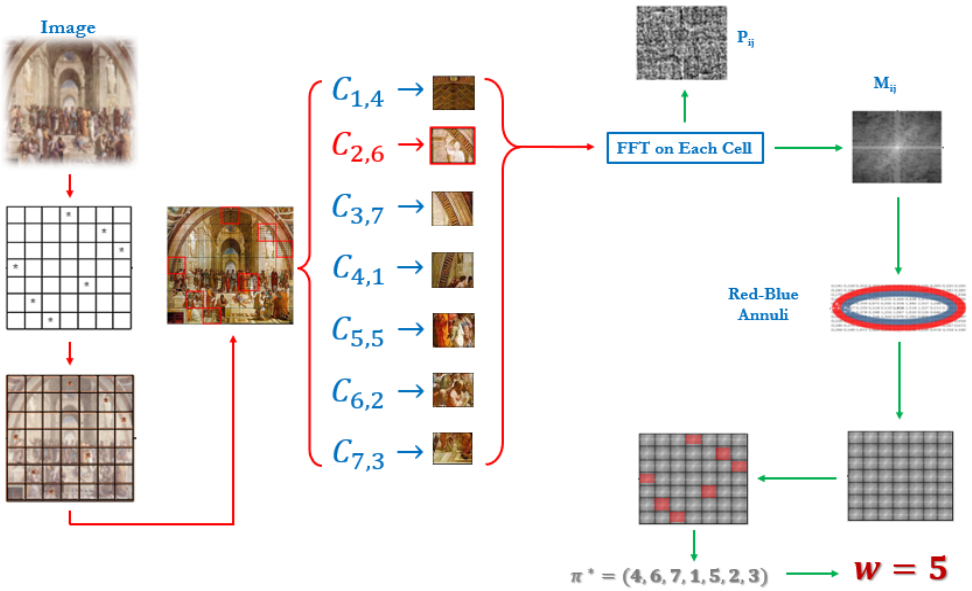


Fig. 2: Extract procedure architecture.

Data: Watermaked Image I_w,
Result: The Integer w that is embedded in I_w
Construct 2DM representations of $Sip(w)$;
for *marked cell in the 2DM representations* **do**
  Select the corresponding cells in I_w;
  for *cell selected from* I_w, *let* $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$ **do**
    Construct 2DM representations of $Sip(w)$;
    for *marked cell in the 2DM representation* **do**
      select the corresponding cells in $C_{i,\pi^*(i)}$;
      for $i = 1$ *to* $i = \ell(\pi^*)$ **do**
        Compute the FFT on this cell;
        Extract the corresponding *magnitude* M_{ij} and *Phase* P_{ij} matrices ;
        Place the Red-Blue Annuli on M_{ij} ;
        For this line select $C'_{i,j} : Avg_{B_{ij}} - Avg_{A_{ij}} = min\{Avg_{B_{ij}} - Avg_{A_{ij}}\}_{j=1}^{j=\ell(\pi^*)}$;
        Construct the SiP;
      end
    end
  end
  Decode the embedded integer w;
end

Algorithm 2: Extraction Algorithm utilizing the extraction approach proposed in [2].

2) then, similarly to the embed procedure. repetitively, for each cell $C_{i,j}$ we utilize again the 2DM representations of the SiP that encodes w, in order to find the marked cells $C'_{i,j}$ inside the boundaries of $C_{i,j}$ and extract the watermark and finally decode it to integer w.

In Algorithm 2, we present step-by-step the procedure of extracting repetitively a watermark into and image utilizing the proposed approach. To this point it is worth noting that the proposed approach ensures that the extraction of at least one of the embedded watermarks is adequate to the ensure the credentials of the author of image I. For the extract procedure we utilize again the 2DM representation of the SiP, which encoded the integer w that embedded into the image I_w, to determine the cells of the image that contain the embedded watermarks. As we can observe from the illustrative example presented in Figure 2 the 2DM representation of the SiP, which encoded the integer w that is embedded in each of the watermarks of I_w is utilized in order to locate the cells $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$. Then, deploying the repetitive watermarking approach as described from the proposed watermarking scheme, for each one of these cells we repeat the procedure by utilizing again the 2DM representation of the SiP, which encoded the integer w that we want to extract from the image I_w to locate the corresponding cells $C'_{1,\pi^*(1)}, C'_{2,\pi^*(2)}, \dots C'_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$ inside the boundaries of an external cell, let $C_{i,j}$. Finally, following the corresponding extraction procedure described in Section II-A the FFT process is applied for each cell $C'_{1,\pi^*(1)}, C'_{2,\pi^*(2)}, \dots C'_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$ each cell of each region in order to compute the amplitude matrices that will be used to indicate the amplitudes of the selected region. The latest step is repeated over the cells inside the boundaries of each cell $C_{1,\pi^*(1)}, C_{2,\pi^*(2)}, \dots C_{\ell(\pi^*),\pi^*(\ell(\pi^*))}$. Finally, we extract the watermark that corresponds to the SiP that encodes the integer number w that we embedded in the image decoding finally the integer w.

III. Evaluation

The evaluation of the proposed repetitive watermarking scheme, is based on metrics that compare the initial image, say I_s (start) against the watermarked image I_w, or the image that results after some attack on it, say I_a (attacked). Through the series of evaluation experiments we tested the imperceptibility of the embedded watermark, that affects the fidelity of the

(a) people.jpg

(b) horizon.jpg

(c) lighthouse.jpg

(d) elephant.jpg

Fig. 3: Data-set of images

watermarked image, as well as the potentials of extracting the hidden information, i.e., the embedded watermark from the watermarked image when attacks have been deployed on it. Note that the hidden information in terms of the structure of the embedded watermark is valid when the extracted watermark can be decoded to its corresponding integer itself or after the reconstruction procedure. The proposed repetitive watermarking technique is developed in Python 3.10 using the Jupyter framework, and the corresponding evaluation experiments where conducted in a commodity computer with 9^th Gen. Intel $i3$-9500 (6 cores - 6 threads) and 8 GB of RAM running over Windows 10.

A. Evaluation Techniques

Next we present the metrics we utilized for the evaluation of the proposed technique and conduct the comparative study taking into account the exhibited experimental results.

- **Peak to Signal Noise Ratio (PSNR).** The PSNR value indicates the distortion of the watermarked image in decibels (dB) in comparison to the original image as follows:

$$PSNR = 10 \cdot log_{10}\left(\frac{255^2}{MSE}\right), \quad (1)$$

- **Structure Similarity Index (SSIM).** The SSIM metric determines how structurally comparable the watermarked and original images are,utilizing the factors of Luminance (L), Contrast (C), and Structure (S), as follows:

$$SSIM(x, y) = L(I_s, I_a)C(I_s, I_a)S(I_s, I_a), \quad (2)$$

B. Methodology

In the experimental setup followed for the evaluation of the proposed repetitive watermarking technique we distinguish four categories of experiments regarding the crop attack. We tested the crop cases where the crop has been performed vertically, horizontally, either in a side of the image or by cropping an intermediate region taking into account various percentages of crop. Moreover we compare the *PSNR* and *SSIM* values exhibited on the images when they have been watermarked utilizing the SiP technique as proposed in [2], and the repetitive one proposed in this work, after a series of compression attacks. The data-set utilized for the evaluation of our proposed model contains images in jpeg format of dimensions 4096×4096 and 8192×8192 as illustrated in Figure 3.

Moreover, in the evaluation results depicted next in Table II, Table III, Table IV, and Table V, we present the potentials of our proposed repetitive watermarking technique against various types of crop attacks. In particular, we distinguish four types of crop attack, namely:

- *Vertical-Side* crop, where the image is cropped vertically by one side. Various percentages of cropping were tested as shown in Figure 4 where the crop has been performed over a 25%, a 50%, and a 75%,
- *Horizontal-Side* crop, where the image is cropped horizontally by one side. Various percentages of cropping were tested as shown in Figure 5 where the crop has been performed over a 25%, a 50%, and a 75%, respectively,
- *Vertical-Intermediate* crop, where the image is cropped vertically in an intermediate area of the image. Various percentages of cropping were tested as shown in Figure 6 where the crop has been performed over a 25%, a 50%, and a 75%, and the
- *Horizontal-Intermediate* crop, where the image is cropped horizontally in an intermediate area of the image. Various percentages of cropping were tested as shown in Figure 7 where the crop has been performed over a 25%, a 50%, and a 75%, respectively.

C. Results

Next we discuss the achieved results regarding the successful watermark extraction procedure considering the four cropping cases, while it is worth noting that a successful watermark extraction is considered in both cases where the watermark has been extracted at its whole extent or the case where parts of it have been extracted and it can be reconstructed through the corresponding procedure presented in [1].

In Table I, we present the corresponding *PSNR* and *SSIM* values resulted from comparing the images watermarked with the technique proposed in [2] and the repetitive one proposed in this work. We also present the time (in seconds) required for embedding the watermark into an image utilizing the two techniques. As we can observe from the experimental

		SIP [2]			This Work		
IMAGE	**SIZE**	**TIME**	**PSNR**	**SSIM**	**TIME**	**PSNR**	**SSIM**
people	4096×4096	2307,12	33,85	0,88	84,14	33,35	0,84
horizon	4096×4096	2309,75	40,79	0,97	83,87	39,28	0,97
lighthouse	8192×8192	18636,07	34,62	0,88	513,7	34,49	0,87
elephant	8192×8192	18297,71	39,23	0,97	504,5	38,42	0,96

TABLE I: Images and watermarking embed time (in seconds), and the metrics that declare the imperceptibility of the corresponding techniques between the image watermarked using each technique against the original one.

(a) 0% (b) 25% (c) 50% (d) 75%

Fig. 4: Vertical-Side Crop

Image	**Cropped** (%)	**[2]**	**This Work**
people	25%	✓	✓
horizon	25%	✓	✓
lighthouse	25%	✓	✓
elephant	25%	✓	✓
people	50%	✓	✓
horizon	50%	✓	✓
lighthouse	50%	✓	✓
elephant	50%	✓	✓
people	75%	✓	✓
horizon	75%	✓	✓
lighthouse	75%	✓	✓
elephant	75%	✓	✓

TABLE II: Extraction results (Vertical-Side crop).

(a) 0% (b) 25% (c) 50% (d) 75%

Fig. 5: Horizontal-Side Crop

Image	**Cropped** (%)	**[2]**	**This Work**
people	25%	✓	✓
horizon	25%	✓	✓
lighthouse	25%	✓	✓
elephant	25%	✓	✓
people	50%	✓	✓
horizon	50%	✓	✓
lighthouse	50%	✓	✓
elephant	50%	✓	✓
people	75%	✗	✓
horizon	75%	✗	✓
lighthouse	75%	✗	✓
elephant	75%	✗	✓

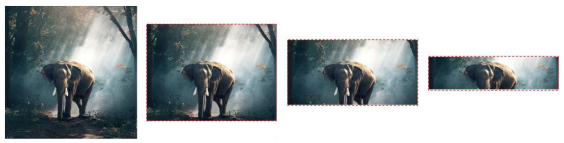
TABLE III: Extraction results (Horizontal-Side crop).

(a) 0% (b) 25% (c) 50% (d) 75%

Fig. 6: Vertical-Intermediate Crop

Image	**Cropped** (%)	**[2]**	**This Work**
people	25%	✗	✓
horizon	25%	✗	✓
lighthouse	25%	✗	✓
elephant	25%	✗	✓
people	50%	✗	✓
horizon	50%	✗	✓
lighthouse	50%	✗	✓
elephant	50%	✗	✓
people	75%	✓	✓
horizon	75%	✗	✓
lighthouse	75%	✓	✓
elephant	75%	✓	✓

TABLE IV: Extraction results (Vertical-Intermediate crop).



(a) 0% (b) 25% (c) 50% (d) 75%

Fig. 7: Horizontal-Intermediate Crop

Image	**Cropped** (%)	**[2]**	**This Work**
people	25%	✓	✓
horizon	25%	✓	✓
lighthouse	25%	✓	✓
elephant	25%	✓	✓
people	50%	✓	✓
horizon	50%	✓	✓
lighthouse	50%	✓	✓
elephant	50%	✓	✓
people	75%	✓	✓
horizon	75%	✓	✓
lighthouse	75%	✓	✓
elephant	75%	✓	✓

TABLE V: Extraction results (Horizontal-Intermediate crop).

Image	[2]	PSNR	SSIM	This Work	PSNR	SSIM
people	✓	33.7	0.87	✓	33.2	0.84
horizon	✓	40.4	0.96	✓	39.0	0.96
lighthouse	✓	34.5	0.88	✓	34.4	0.86
elephant	✓	39.2	0.96	✓	38.3	0.95

TABLE VI: Compression attack (quality= 90%).

Image	[2]	PSNR	SSIM	This Work	PSNR	SSIM
people	✓	33.4	0.86	✓	33.01	0.82
horizon	✓	40.02	0.96	✓	38.7	0.96
lighthouse	✓	34.5	0.87	✓	34.3	0.86
elephant	✗	39.1	0.96	✓	38.2	0.95

TABLE VII: Compression attack (quality= 80%).

Image	[2]	PSNR	SSIM	This Work	PSNR	SSIM
people	✓	33.2	0.85	✓	32.8	0.82
horizon	✓	39.5	0.96	✓	38.3	0.95
lighthouse	✗	34.4	0.87	✓	34.3	0.86
elephant	✗	39.1	0.96	✓	37.9	0.95

TABLE VIII: Compression attack (quality= 70%).

results depicted in Table I, the time required by the repetitive watermarking technique proposed in this work is significantly faster (97.1%) against the one proposed in [2], while the corresponding *PSNR* and *SSIM* values are almost equal.

The observation regarding the reduction in the time required for embedding procedure results from the fact that the repetitive technique encodes the watermark in less DFT coefficients. More precisely, in the case of an image of dimensions 4096×4096 the initial watermarking technique proposed in [2] processes 49 cells of dimensions 585×585 pixels, while the repetitive watermarking technique proposed in this work, processes 7 cells of dimensions 585×585 pixels, that each contains 49 cells of dimensions 83×83 pixels. Finally, the technique proposed in [2], results in processing 16.769.025 DFT coefficients, while the technique proposed in this work processes only 2.362.972, i.e. 85.9% reduction in processing cost. Similarly, in the case of an image of dimensions 8192×8192, the initial watermarking technique proposed in [2], processes 49 cells of dimensions 1170×1170 pixels, while the repetitive watermarking technique proposed in this work, processes 7 cells of dimensions 1170×1170 pixels, that each contains 49 cells of dimensions 167×167 pixels. The technique propose in [2], in the case of an image of dimensions 8192×8192 results in the processing of 67.076.100 coefficients, while the technique proposed in this work, processes only 9.565.927, i.e. 85.7% reduction in processing cost.

As we can observe from the results depicted Table II regarding the attack of Vertical-Side crop, where the image is cropped vertically by one side, all images regardless the percentage of cropping, achieve to extract the embedded watermark successfully in both techniques, i.e. the proposed in [2] and the repetitive watermarking technique proposed in this work. Similarly, for the case of Horizontal-Side crop, where the image is cropped horizontally by one side, as we can observe from the results depicted Table III, both techniques, achieve to successfully extract the embedded watermark for crops of 25% and 50%, while for crops of size 75% the technique proposed in [2] fails to extract the embedded watermark.

Moreover, considering the cases of Vertical-Intermediate and Horizontal-Intermediate crop, as we can observe from the results depicted in Table IV considering the case of Vertical-Intermediate crop, where the image is cropped vertically in an intermediate area of the image, the technique proposed in [2] fails to extract the embedded watermark, while the repetitive watermarking technique proposed in this work achieves a successful watermark extraction, i.e., by extracting the whole watermark or reconstruct it by the extracted parts of it in all the cases. However, considering the case of Horizontal-Intermediate crop, where the image is cropped horizontally in an intermediate area of the image, both the technique proposed in [2] and the repetitive watermarking technique proposed in this work, achieve a successful watermark extraction, i.e., by extracting the whole watermark or reconstruct it by the extracted parts of it in all the cases. To this point we should underline that the potentials of the repetitive watermarking technique are depicted by the fact that in all the cases of cropping regardless the amount of the cropped image, i.e., even in the extreme case where only an 25% of the image has been left to contain the hidden information, the proposed repetitive watermarking scheme is able to extract successfully the hidden information.

On the other hand, considering the compression attacks, we distinguish three cases regarding the quality of the watermarked image that has been compressed. In particular, we distinguish three compression qualities, i.e., 90%, 80%, and 70%. In Table VI we present the extraction results after the compression attack with quality= 90%, in Table VII we present the extraction results after the compression attack with quality= 80%, while in Table VIII we present the extraction results after the compression attack with quality= 70%. In all the cases we consider again the successful extraction of the embedded watermark through the deployment of the initial watermarking technique proposed in [2] and the repetitive watermarking scheme proposed in this work, as also the exhibited *PSNR* and *SSIM* values. As we can observe from the experimental results depicted through the corresponding tables, our proposed technique proves its imperceptibility and robustness against the compression attack even for higher compression that indicate lower quality of the watermarked image. The achieved results show that the repetitive watermarking scheme proposed in this work is comparable to the baseline proposed in [2] and in many cases it shows significant improvements.

Finally, in Table IX we present the percentages of the cases of successful watermark extraction after the performance of the corresponding attack. In particular, the percentages presented in Table IX depict the number of cases where each watermarking technique achieved to extract successfully w, i.e., either the whole watermark embedded or by reconstructing it

	Vertical-Side	Horizontal-Side	Vertical-Intermediate	Horizontal-Intermediate	Comp. 90%	Comp. 80%	Comp. 70%
SIP [2]	100%	25%	100%	66%	100%	75%	50%
This Work	100%	100%	100%	100%	100%	100%	100%

TABLE IX: Comparative results after crop and compression attacks.

utilizing the extracted segments. Comparing the experimental results exhibited through the evaluation of our proposed model regarding the repetitive watermarking of digital images with to the baseline, as we can observe from Table IX in any case after the performance of the corresponding attack the repetitive watermarking scheme proposed in this work achieves an 100% successful watermark extraction, where the initial technique proposed in [2] failed to even reconstruct the embedded watermark by the segments extracted after the corresponding attack, that indeed shows the improvement achieved through the proposed approach.

IV. Conclusion

In this work, we presented a novel watermarking scheme based on the repetitive embed of watermarks by the utilization of Self-inverting Permutations. In particular we utilized the approach proposed in [2] that provide the 2DM representations of a SiP that encodes an integer, where for these specific cells we repetitively apply the corresponding 2DM representation that encodes the same integer to embed the watermark repetitively into these cells. The multiple watermark embedding into different areas of the image guarantee that in the watermarked image retains its imperceptibility while it is even more robust against crop attacks, where even with an 25% of the image available the proposed technique achieve to extract the embedded watermark successfully. Moreover, the proposed repetitive watermarking technique is applied faster than the baseline while a 97% reduction in the required time has been achieved for the embedding procedure and an average of 85.8% reduction in the corresponding processing cost.

A. Remarks

The repetitive watermarking technique proposed in this work achieved equal *PSNR* and *SSIM* values compared to the base line while it achieved a successful extraction of the hidden information, i.e., the watermark, in all the crop attacks which prove its potentials compared to the baseline that particularly in the cases of vertical and horizontal crops when they performed in intermediate parts of the image failed to extract the embedded watermark. Moreover, the proposed technique, for the case of crop attacks, achieved to extract at least one watermark at its whole extent without reconstructing it, while in the case of compression attacks for a compression quality of 90% and 80% it extracted the whole watermark where for a compression quality of 70% it achieved to reconstruct the extracted watermark successfully, that is also a point worth noting.

B. Future Research

The experimental evaluation results show that the proposed repetitive watermarking technique exhibits adequate imperceptibility and robustness especially for the case of crop attacks. These findings guide our future research aims on further investigation of the properties exhibited by the repetitive watermarking scheme regarding its structure and the type of information embedded in the image. Additionally, more complex attacks could be designed in order to prove its potentials against elaborated tamper techniques.

Acknowledgment

This research was supported by project "Dioni: Computing Infrastructure for Big-Data Processing and Analysis" (MIS No. 5047222) co-funded by European Union (ERDF) and Greece through Operational Program "Competitiveness, Entrepreneurship and Innovation", NSRF 2014-2020.

References

[1] Chroni, M., Nikolopoulos, S. D., and Palios, L.: Encoding watermark numbers as reducible permutation graphs using self-inverting permutations. Discrete Applied Mathematics, 250, 145-164, (2018).

[2] Chroni, M., Fylakis, A., and Nikolopoulos, S. D.: Watermarking images in the frequency domain by exploiting self-inverting permutations. WEBIST 2013, 45-54, (2013).

[3] Vaidya, S. P., and Kishore, V. R.: Adaptive Medical Image Watermarking System For E-Health Care Applications. SN Computer Science, 3(2), 1-10, (2022).

[4] Sinhal, R., Jain, D. K., and Ansari, I. A.: Machine learning based blind color image watermarking scheme for copyright protection. Pattern Recognition Letters, 145, 171-177, (2021).

[5] Fares, K., Khaldi, A., Redouane, K., and Salah, E.: DCT and DWT based watermarking scheme for medical information security. Biomedical Signal Processing and Control, 66, 102403 (2021).

[6] Yuan, Z., Su, Q., Liu, D., and Zhang, X.: A blind image watermarking scheme combining spatial domain and frequency domain. The Visual Computer, 37(7), 1867-1881,(2021).

[7] Malayil, M. V., and Vedhanayagam, M.: A novel image scaling based reversible watermarking scheme for secure medical image transmission. ISA transactions, 108, 269-281, (2021).

[8] Gong, L. H., Tian, C., Zou, W. P., and Zhou, N. R.: Robust and imperceptible watermarking scheme based on Canny edge detection and SVD in the contourlet domain. Multimedia Tools and Applications, 80(1), 439-461, (2021).

[9] Mellimi, S., Rajput, V., Ansari, I. A., and Ahn, C. W.: A fast and efficient image watermarking scheme based on Deep Neural Network. Pattern Recognition Letters, 151, 222-228, (2021).

[10] Moad, M. S., Kafi, M. R., and Khaldi, A.: A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocessors and Microsystems, 90, 104490, (2022).

[11] Yan, F., Huang, H., and Yu, X.: A multi-watermarking scheme for verifying medical image integrity and authenticity in the Internet of Medical Things. IEEE Transactions on Industrial Informatics (2022).

[12] Faheem, Z. B., Ali, M., Raza, M. A., Arslan, F., Ali, J., Masud, M., and Shorfuzzaman, M.: Image Watermarking Scheme Using LSB and Image Gradient. Applied Sciences, 12(9), 4202, (2022).