Robust Image watermarking Method Using Homomorph Block-Based KLT

Hanaa a. Abdallah a, Osama S. Faragallah b,f,*, Hala S. Elsayed c, Mohiy M. hadhoud d, Abdalhameed A. Shaalan a, Fathi E. Abd El-samie e

a Faculty of Engineering, Zagazig university, Zagazig, Egypt
b Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
c Department of Electrical Engineering, Menoufia University, 32511 Shebin El-kom, Egypt
d Faculty of computers and information, Menoufia University, Shebin Elkoom, Egypt
e Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
f Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Kingdom of Saudi Arabia

ARTICLE INFO

Article history:
Received 23 December 2014
Accepted 11 October 2015

Keywords:
Watermarking
Homomorphic transform
KLT
Copyright protection

ABSTRACT

This paper introduces two robust image watermarking methods using a combination of homomorphic transform and Karhunen Loeve Transform (KLT). The first proposal is denoted as homomorphic-based KLT image watermarking. It works by inserting the watermark during applying the KLT to the reflectance component estimated from employing the homomorphic transform on the host image that will be watermarked. The reflectance component includes significant merits of image, so the embedded watermark with this component is immune to various types of attacks. The second proposal is denoted as homomorphic block-based KLT image watermarking. It works by segmenting the reflectance component of the host image into blocks using spiral scan and adding the watermark to every block during the application of the KLT to each block, separately. The watermark addition using block-by-block principle strengthens the watermark and makes it more immune to attacks. The two proposed methods are compared with homomorphic-based Singular Value Decomposition (SVD) image watermarking method, homomorphic block-based SVD image watermarking method, the traditional SVD watermarking method, and other image watermarking methods. Experimental results ensure that the two proposed methods are immune and secure to different attacks like cropping, scaling, JPEG compression and Gaussian noise without degrading the watermarked image to the same level as the other techniques.

© 2015 Elsevier GmbH. All rights reserved.

1. Introduction

Digital multimedia like images, audio, and video are vulnerable to tampering, replication, and spreading through communication networks. These communication networks may be public and open for external manipulation of the transmitted signals or information. This may raise some issues like copyright protection. The copyright protection is a very essential issue in several applications.

Digital watermarking is suggested to recognize the holder and spreading pathway of digital multimedia. Watermarking is a means of inserting unobserved owner information to digital multimedia by performing tiny changes to multimedia data. Various image watermark schemes have been suggested. Several schemes work by changing spatial or temporal data samples [1–3], however others work by changing transform coefficients [4–10]. In contradiction to encryption, watermarking schemes allow access to the data. A watermark is prepared to always remain within the cover data. The data owner proves his royalty by extracting the information to ensure the ownership or delivery path.

Image watermarking schemes using SVD have been widespread because of the significant mathematical characteristics of the SVD and its easy implementation. With respect to SVD-based image watermarking, many schemes may be employed [11–17]. A popular scheme may apply the SVD to the host image, and change all the SVs to attach the watermark. A significant feature of SVD-based watermarking is that almost SVs are not affected by most attacks.

Efficient image watermarking methods must guarantee the robustness and the imperceptibility of the digital multimedia. The imperceptibility is the visual similarity between the host and
watermarked images which is a significant tool used to evaluate the strength of the watermarking technique. Robustness estimates the resistance of the watermarking technique to various attacks.

The main paper objective can be concluded through introducing two efficient combined homomorphic-KLT watermarking schemes that ensure both robustness and imperceptibility of digital images. The first method embeds the watermark throughout performing the KLT on the host image reflectance component. The second method divides the reflectance component of the host image into blocks using spiral scan and performs the KLT to each block and embeds the watermark into the transform.

If we look at the image in the homomorphic domain, the image reflectance component has the most significant features, and embedding the watermark in this component guarantees immunity to various attacks. Segmentation of the reflectance component of the host image with spiral scan ensures the robustness of the suggested watermarking method since, the watermark is embedded with more than one block, which enhances the watermarking scheme immunity to various attacks. The KLT has two significant features; the feature of signal dependency and conversion to real functions [4-5]. These features confirm the KLT applicability for robustness watermarking [6]. The obtained results demonstrate that the two proposed watermarking methods are not only immune to popular image processing operations like JPEG compression, noise addition, and blurring etc., but also immune to desynchronization attacks like scaling, cropping, and rotation, etc. The rest of the paper is arranged as follows. Section 2 explores image watermarking types. Section 3 discusses the related work of transform domain based SVD watermarking. Section 4 introduces the proposed KLT watermarking in the homomorphic domain. Section 5 introduces the proposed block-based KLT watermarking in the homomorphic domain. Section 6 explores simulation results. Section 7 gives a comparison between the proposed homomorphic-based KLT image watermarking, the homomorphic block-based KLT image watermarking, and other image watermarking schemes. Section 8 gives conclusions.

2. Image watermarking

There are two types of watermarking; watermarking of the image as a whole and block-based watermarking.

2.1. Watermarking of the image as a whole

Tan and Liu have introduced an algorithm that directly embeds the watermark to the whole image in the SVD domain [11]. This algorithm requires orthogonal matrices or the SVs for recovering the watermark. It is immune to several attacks like cropping, filtering, and compression, but it is not robust to attacks containing translation and rotation.

Kong and Liu have also proposed an algorithm based on SVD. Their algorithm utilizes an M-sequence as the watermark. Taking into account the robustness and quality criteria, the process starts by adding the watermark to the middle coefficients of SVs keeping the original order. This scheme belongs to the blind category which does not need the source data or image of the source SVs for watermark detection. This algorithm can survive several attacks such as median filtering, Gaussian LPF, JPEG compression and rescaling, while it is not robust enough to some other attacks containing cropping and rotation.

2.2. Block-based watermarking

Ganic et al. [14] suggested an SVD technique that adds the watermark twice. The host image is firstly broken into blocks (layer 1) and each block is processed by embedding a segment of the watermark. The host image is treated as a single block to add the entire watermark in the 2nd layer. The 1st layer gives flexibility for the capacity of the data, while the 2nd layer gives extra robustness to attacks. This technique can survive various attacks like Gaussian noise, Gaussian blur, JPEG 2000, JPEG compression, rotation, cropping and rescaling. Moreover, The visual quality is distorted after each attack and the image loses its commercial importance. Regarding the rotation attack, experiments have reported the small angle only. Also, this technique lacks the robustness against translation attack.

Ghazi et al. [15] have suggested a SVD based technique, where the cover image is segmented into blocks. Thereafter, for each block, the SVs are embedded by the watermark. An image or a pseudo random number can be used as a watermark. This technique can survive attacks like Gaussian noise, JPEG compression, cropping, Gaussian blur, rotation and resizing, and the correlation value for resizing and rotation has bad result. Also, this technique is not immune to translation attack.

Zhou et al. [16] have suggested a technique in which the cover image is broken into several non-overlapping blocks of size 8 × 8 and for each block, the SVD is computed and the watermark is added in the SVD domain. A gray-scale image, a pseudo random number, or a binary image could be the watermark to be added. A prior step is required to adjust the host image size if it is not exactly divisible by 8 before adding the watermark. Results revealed that the technique is immune to noise, rotation, clipping, JPEG compression, and filtering. Also, the correlation coefficient is evaluated for the original and extracted watermarks which may indicate an unsatisfactory value for rotation attack. In addition, the immunity of this technique to scaling and translation attacks is not good.

3. Transform domain based SVD watermarking

Some algorithms have been presented for SVD watermarking in transform domains.

3.1. DCT-based SVD watermarking

Sverdlov et al. [17] suggested a DCT-based SVD watermarking method. The entire cover image is converted to DCT domain, and the coefficients of DCT are divided into four parts using a zigzag sequence, then the SVD is evaluated for each part. In fact, these four parts represent frequency bands and are arranged from the lowest to the highest. The watermark is transformed to DCT domain, then the SVs are evaluated and used to change the SVs of each part of the host image. Results have illustrated that embedding the watermark in the highest frequencies can resist some types of attacks, while embedding the watermark in the lowest frequencies can resist other types. The algorithm has been examined in terms of robustness for various attacks such as JPEG compression, rescaling, Gaussian blur, cropping, JPEG 2000 compression, gamma correction, Gaussian noise, and histogram equalization. The results illustrated that the algorithm is not immune to translation attack and the robustness to rotation attack is uncertain.

3.2. DWT-based SVD watermarking

Ganic and Eskicioglu [14] proposed a DWT-based SVD watermarking algorithm. This algorithm is very close to the algorithm in [17]. The host image is transformed to DWT with four sub-bands and the SVD is evaluated for each sub-band. Also, the SVD of the watermark image is evaluated and the SVs of the watermark modify the SVs of the host image. The modified four sets of DWT coefficients are inversely transformed to obtain the watermarked image. The
algorithm has been examined in terms of robustness for various attacks like JPEG compression, rescaling, Gaussian blur, cropping, JPEG 2000 compression, gamma correction, Gaussian noise, and histogram equalization. The results revealed that the best watermark in correlation coefficient and visual quality is extracted from the LL band. Attacks such as histogram equalization, contrasting and sharpening revealed that the performance of this algorithm was bad.

3.3. Hadamard-based SVD watermarking

The SVD watermarking used the Fast Hadamard Transform (FHT) [18]. The algorithm starts by breaking the host image into segments and the FHT is applied to every segment. Then, SVD is evaluated for the watermark image and their SVs are distributed along the transformed host blocks. This algorithm is characterized by real time implementation, flexibility in data embedding capacity, and simplicity. The scheme has been examined in terms of robustness for various attacks such as resizing, Gaussian blur, rotation, cropping, gamma correction, Gaussian noise, and histogram equalization. Attacks including translation have not been tested, which reveals a weakness of this algorithm.

3.4. Zernike moments-based SVD watermarking

Zernike moments-based SVD watermarking technique has been suggested by Li et al. [19]. It is known that the Zernike moments are rotation invariant. So, they are utilized to evaluate the rotation angle to ensure that the algorithm acquires the rotation invariant property. The host image is segmented and the SVD is evaluated for every block. The results have revealed that the robustness of this algorithm against rotation, pixel removal and scaling attacks is good. The normalized correlation is used to estimate the similarity between the source and the extracted watermark, while the Weighted Peak Signal-to-Noise Ratio (WPSNR) is employed to estimate the visual quality of the watermarked image.

4. The Proposed Homomorphic-Based KLT Image Watermarking Method

This section explores the first proposed watermarking method denoted as homomorphic-based KLT image watermarking. The image is represented as a 2-D function and takes the form $G(x,y)$, whose light intensity values in spatial coordinates $(x,y)$ are positive quantities [20]. The pixels intensity can be represented by multiplying reflectance and illumination components. The illumination component is considered fixed and the reflectance component contains utmost details. The reflectance component is generated by the method the image reflects light, and can be estimated from the object intrinsic properties. For this reason, the watermark is expected to be embedded in the reflectance component to resist different attacks [20]. Detailed steps for embedding the watermark in the image reflectance component using KLT and detecting the watermark are explored below.

4.1. Watermark embedding

1. The pixels intensity of an image $G$ can be represented as [20]:

$$G(x, y) = I(x, y) \times R(x, y) \quad (1)$$

where $I(x,y)$ and $R(x,y)$ are the object illumination component matrix and reflectance component matrix, respectively.

2. The homomorphic transform is applied to $G(x,y)$.

$$\ln[G(x, y)] = \ln[I(x, y)] + \ln[R(x, y)] \quad (2)$$

3. A Low pass filter (LPF) and a High pass filter (HPF) are performed on $\log[G(x,y)]$ to extract the illumination and reflectance component matrices, respectively.

4. The KLT [4-6] is applied to the reflectance component matrix $R(x,y)$. The KLT converts the image reflectance component matrix to an image of statistically independent components. The watermark is embedded through the transformation process. The KLT can be represented as [4-6]:

$$[\text{KLT}] = V \times R \quad (3)$$

where $V$ represents the eigenvector matrix extracted from the reflectance component $R$.

5. The watermark ($W$ matrix) is embedded to the KLT of the reflectance component matrix $[\text{KLT}]$.

$$D = [\text{KLT}] + W \quad (4)$$

6. The inverse KLT is applied as follows:

$$R_w = [\text{IKLT}] = V^T \times D \quad (5)$$

where $V^T$ represents the transpose of the eigenvector matrix.

7. The inverse homomorphic transform is applied to $I$ and $R_w$ to obtain the matrix $Y_w$.

$$Y_w = R_w + I \quad (6)$$

8. The watermarked image $G_w$ is obtained using:

$$G_w = \exp(Y_w) \quad (7)$$

4.2. Watermark detection

The watermark extraction process is employed for detecting a possible distorted watermark from a possible corrupted watermarked image, given the watermark $W$, and a possible corrupted watermarked image $G_w$. The above-mentioned steps are employed in a reverse order as:

1. Perform homomorphic transform to the original and watermarked images $G$ and $G_w$.

2. Utilize a high pass filter to obtain the original and possibly distorted reflectance component matrices $R$ and $R_w$.

3. Apply the KLT to the original and possibly distorted reflectance component matrices $R$ and $R_w$.

$$[\text{KLT}1] = V \times R \quad \text{and} \quad D^* = [\text{KLT2}] = V \times R_w \quad (8)$$

4. The possibly distorted watermark $W^*$ is obtained.

$$W^* = D^* - [\text{KLT}1] \quad (9)$$

5. The Proposed Homomorphic Block-Based KLT Image Watermarking Method

5.1. Watermark embedding

The steps from 1 to 3 as in Section 4.1 are performed, and then:

4. Segment the reflectance components matrix $R$ into blocks $R_i$ utilizing spiral scan as depicted in Fig. 1.

5. Apply the KLT to each block $R_i$ of the reflectance component matrix $R$. The KLT converts the reflectance component block to a block of statistically independent components. The watermark is embedded through the transformation process. The KLT can be represented as:

$$[\text{KLT}]= V_i \times R_i \quad (10)$$

where $V_i$ represents the eigenvector matrix extracted from the reflectance component block $R_i$. 
The watermark (W matrix) of the same block size is embedded to the KLT of the reflectance component block [KLTi].

\[ D_1 = [KLT_i] + W \]  \hspace{1cm} (11)

7. Apply the inverse KLT, where the IKLT is represented as:

\[ R_{wi} = [IKLT_i] = V_i^T \times [KLT_i] \]  \hspace{1cm} (12)

where \( V_i^T \) represents the transpose of eigenvector matrix.

8. Perform the previous steps 5-7 for all reflectance component matrix blocks.

9. Combine the watermarked reflectance component blocks \( R_{wi} \) into one watermarked reflectance component matrix \( R_w \) in order to construct the watermarked image \( G_w \).

The steps 7-8 are performed as in Section 5.1.

5.2. Watermark detection

The steps 1-2 in Section 4.2 are performed and then:

3. Segment the original and watermarked reflectance components matrices \( R \) and \( R_w \) into segments \( R_i \) and \( R_{wi} \) of equal size as utilized in the embedding procedure and utilizing the same method of spiral scan.

4. Apply the KLT to each block \( R_i \) and \( R_{wi} \) of the original and watermarked reflectance component matrices.

\[ [KLT1_i] = V_i \times R_i \] and \[ D_i^* = [KLT2_i] = V_i \times R_{wi}^* \]  \hspace{1cm} (13)

5. The possibly distorted watermark \( W_i^* \) is obtained.

\[ W_i^* = D_i^* - [KLT1_i] \]  \hspace{1cm} (14)

The * refers to the corruption due to attacks. Embedding and detection are shown in Figs. 2-3.

6. Simulation results

This section presents experimental results, which are performed on the two proposed homomorphic-based KLT image watermarking and homomorphic block-based KLT image watermarking methods. The 512×512 gray-scale Lena and the 512×512 colored Flowers images are employed to carry out the simulation experiments. The three color channels in RGB color system are highly correlated making this system not appropriate for watermarking applications. There is an exception with respect to blue channel due to its weak impact on the human eye [21]. So, it is required to convert the RGB color system to another color system whose channels are not correlated. We have adopted the Y Cb Cr color system because nearly all the data is saved in the Y channel (luminance) and
the rest of the data is in the Cb and Cr channels (chrominance). The experiments demonstrated a more considerable effect on human eye, when embedding the watermark in Y channel than in the Cb and Cr channels. But, the two proposed image watermarking methods utilize the Y channel to embed the watermark for its robustness to JPEG compression attack. Fig. 4 shows the watermark, the original gray-scale Lena image, the extracted watermark and the watermarked Lena image using the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods. By visual inspection, the results reveal that no noticeable variations exist between the watermarked and original images, which enforces the fidelity of the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods. The estimated PSNR for the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods equals 49.03 dB and 51.73 dB, respectively. The computed correlation coefficients between the original and extracted watermarks from the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods are 0.93 and 0.99, respectively.

Attacks such as compression, resizing, rotation, cropping, and Gaussian noise are performed on the watermarked images. The original and extracted watermarks under attacks are shown in Figs. 5 and 6 for the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods. Firstly, the JPEG compression attack is applied. Secondly, resizing from 512 to 256 and back to 512 again attack is applied. Thirdly, Gaussian noise addition with zero mean and 0.15 variance attack is applied. Fourthly, the cropping attack is applied. Finally, rotating with (-30°) attack is applied. Fig. 5 illustrates the restored watermarks and the correlation coefficient between the original and restored watermarks for different attack types for the proposed homomorphic-based KLT image watermarking method. Results illustrate that the Cr value is greater than 0.62, which guarantees watermark existence. The figures reveal the superiority in restoring watermarks with the existence of powerful attacks for the first proposed homomorphic-based KLT watermarking image method. The restored watermarks for the second proposed homomorphic block-based KLT image watermarking method after applying the same attacks are shown in Fig. 6. For all results, there are restored watermarks with Cr greater than 0.95, which guarantees watermark existence. The figures indicate the superiority of the second proposed homomorphic block-based KLT image watermarking in the presence of cropping, compression, and Gaussian noise attacks. Figs. 7 to 9 depict the simulation results for the colored Flowers image with size $512 \times 512$ by the two proposed homomorphic-based KLT and homomorphic block-based KLT watermarking methods.

Fig. 5. Watermarks extracted using the proposed homomorphic-based KLT method after applying attacks for the gray scale Lena image.
7. Comparison Study

To correctly examine the performance of the two proposed image watermarking methods, a comparison is performed between the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods against six image watermarking algorithms. Firstly, Liu et al. [11] is considered as a reference method, which is based on singular value decomposition (SVD). We call it as Liu_method, which inserts the watermark in the entire cover image in the SVD domain. The method utilizes the SVs matrices for obtaining the watermark. The second method is denoted as wavelet-based watermarking method [22]. It depends on sorting the wavelet coefficients as effective or ineffective by zerotree, and then inserts the watermark into the place of ineffective coefficients or into the place of threshold effective coefficients at the coarser scales. The third method is known as the DWT-based SVD watermarking [23]. It works by decomposing the cover image with the DWT into four sub-bands, then for each band, the SVD is computed. The SVs of the watermark image change the SVs of the host image. We name the fourth method as the DWT-based chaotic watermarking. It depends on adding a binary watermark pattern after performing a chaotic mixing method in the DWT domain [24]. The fifth method is known as homomorphic-based SVD. It works by adding the watermark with the SVD algorithm in the reflectance component after employing the homomorphic transform on the host image [8]. The sixth method is known as homomorphic block-based SVD image watermarking. It works utilizing the SVs after segmenting the host image into blocks to embed the watermark to every block, separately [8]. The 512 × 512 gray-scale Lena and colored Flowers images have been employed in experiments. The normalized correlation between the coefficients of the original watermark and the transform coefficients of the extracted watermark is measured by the watermark decoder. The normalized correlation is computed for all methods of the watermarked sequence which has never suffered from any kind of distortion. All the six watermarking methods have the ability to detect each.

![Image](https://via.placeholder.com/150)

**Fig. 6.** Watermarks extracted using the proposed homomorphic block-based KLT method after applying attacks for the gray scale Lena image.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>0.8500</td>
<td>0.8800</td>
<td>0.8920</td>
<td>0.9073</td>
<td>0.9153</td>
<td>0.9760</td>
<td>0.93</td>
<td>0.99</td>
</tr>
<tr>
<td>JPEG compression Q=60%</td>
<td>0.6015</td>
<td>0.6160</td>
<td>0.6420</td>
<td>0.6660</td>
<td>0.6950</td>
<td>0.9640</td>
<td>0.71</td>
<td>0.98</td>
</tr>
<tr>
<td>Resizing 512–256–512</td>
<td>0.5714</td>
<td>0.6120</td>
<td>0.6340</td>
<td>0.6500</td>
<td>0.6615</td>
<td>0.9530</td>
<td>0.67</td>
<td>0.97</td>
</tr>
<tr>
<td>Gaussian noise with variance=0.15</td>
<td>0.1438</td>
<td>0.3120</td>
<td>0.5780</td>
<td>0.5960</td>
<td>0.6190</td>
<td>0.8920</td>
<td>0.63</td>
<td>0.96</td>
</tr>
<tr>
<td>Cropping Rotation (-3°)</td>
<td>0.3017</td>
<td>0.5480</td>
<td>0.7170</td>
<td>0.7350</td>
<td>0.7634</td>
<td>0.9410</td>
<td>0.79</td>
<td>0.98</td>
</tr>
<tr>
<td></td>
<td>0.1747</td>
<td>0.2310</td>
<td>0.3560</td>
<td>0.4820</td>
<td>0.6654</td>
<td>0.9470</td>
<td>0.74</td>
<td>0.97</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>0.8780</td>
<td>0.8940</td>
<td>0.8990</td>
<td>0.9090</td>
<td>0.9170</td>
<td>0.9650</td>
<td>0.93</td>
<td>0.99</td>
</tr>
<tr>
<td>JPEG compression Q=60%</td>
<td>0.6379</td>
<td>0.6680</td>
<td>0.6865</td>
<td>0.7020</td>
<td>0.7230</td>
<td>0.9660</td>
<td>0.75</td>
<td>0.98</td>
</tr>
<tr>
<td>Resizing 512–256–512</td>
<td>0.594</td>
<td>0.6290</td>
<td>0.6480</td>
<td>0.6520</td>
<td>0.6756</td>
<td>0.9625</td>
<td>0.70</td>
<td>0.97</td>
</tr>
<tr>
<td>Gaussian noise with variance=0.15</td>
<td>0.1965</td>
<td>0.4230</td>
<td>0.6330</td>
<td>0.6480</td>
<td>0.6550</td>
<td>0.9210</td>
<td>0.68</td>
<td>0.96</td>
</tr>
<tr>
<td>Cropping Rotation (-15°)</td>
<td>0.3756</td>
<td>0.6580</td>
<td>0.7960</td>
<td>0.8870</td>
<td>0.8165</td>
<td>0.965</td>
<td>0.83</td>
<td>0.98</td>
</tr>
<tr>
<td></td>
<td>0.1987</td>
<td>0.2758</td>
<td>0.3740</td>
<td>0.5970</td>
<td>0.6960</td>
<td>0.9510</td>
<td>0.77</td>
<td>0.97</td>
</tr>
</tbody>
</table>
Fig. 7. (a) Original Lena image. (b) Watermark. (c) Watermarked image without attacks with the proposed homomorphic-based KLT method with PSNR = 52.72 dB (d) Recovered watermark $c_r = 0.939$ with the proposed homomorphic-based KLT method (e) Watermarked image with the proposed homomorphic block-based KLT method with PSNR = 58.35 dB (f) Recovered watermarks with the proposed homomorphic block-based KLT method (g) Magnification of the watermark with $c_r = 0.995$.

Fig. 8. Watermarks extracted using the proposed homomorphic-based KLT method after applying attacks for the colored Flowers image.

Fig. 9. Watermarks extracted using the proposed homomorphic block-based KLT method after applying attacks for the colored Flowers image.
watermark, correctly. The normalized correlation is computed as follows:

$$\text{Normalized Correlation : } NC(w_{in}, w_{out}) = \frac{\sum_{i,j} w_{in}(i,j) w_{out}(i,j)}{\sum_{i,j} [w_{in}(i,j)]^2}$$  \hspace{1cm} (15)$$

where, $w_{in}$ and $w_{out}$ are the original and extracted watermarks. Tables 1 and 2 give the normalized correlation values for grayscale Lena and colored Flowers test images with all watermarking schemes under various attacks. It is clear that the two proposed homomorphic-based KLT and homomorphic block-based KLT image watermarking methods outperform other schemes [8, 11, 22–24] under most attacks in terms of the normalized correlation between the coefficients of the original watermark and the transform coefficients of the extracted watermark. From Tables 1 and 2, the results demonstrate the achievements of the two proposed watermarking methods utilizing the mixed homomorphic-KLT domains. Also, it is noticeable that the watermark has a high degree of robustness to both common image processing operations and various desynchronization attacks by combining the two proposed block-based KLT and KLT image watermarking methods in the homomorphic domain.

8. Conclusions
The paper proposed two efficient watermarking methods utilizing a combination of homomorphic transform and the KLT. The first proposed homomorphic-based KLT image watermarking method embeds the watermark during employing the KLT to the reflectance component after applying the homomorphic transform to the host image. The second proposed homomorphic block-based KLT image watermarking embeds the watermark through employing the KLT to the HPI output of the homomorphic transform of the host image after splitting it into blocks. It is shown that we can transmit two images, the watermark and host images as a single watermarked image. This can achieve a reduction in bandwidth. The experimental results demonstrated that the homomorphic block-based KLT watermarking has a high fidelity and robustness in the presence of different types of attacks. There is always a large probability for watermark detection. The achieved results also reveal the superiority of the proposed homomorphic block-based KLT image watermarking method over other watermarking schemes.

References