International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 12 | December - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Data Protection Based on Image Watermarking Using Various Decomposition Techniques

R SUDHA RANI
PG STUDENT, ECE DEPARTMENT
BVSR Engineering College, Chimakurthy, A.P INDIA

G V RAVI KUAMR
ASSOCIATE PROFESSOR, ECE DEPARTMENT
BVSR Engineering College, Chimakurthy, A.P.INDIA

***Abstract*—In this paper, data protection based on image watermarking using carious decomposition techniques. Digital watermarking system is widely used for security, data encryption in the real time system. The digital watermarking system is decomposed into various level of sub-bands using various multiresolution system. The watermark image is encrypted into the original input image to provide the watermarked image. It is implemented on the behavior of intellectual things need to applied for protection of the digital watermarking. The feature extraction is purely depends on the least significant bit method. The decomposition method is a robustness of least significant bit to increase the image quality of the system. The proposed method has been successfully implemented on the various real time images to protect the data. The experimental results provides better results as comparted to existing methods.**

Keywords—Digital Watermarking, LSB Embedding, Multimedia Protection, Copyright, Illegal Distribution, Halftone Images, Information Security

I. INTRODUCTION

The task of protection of digital multimedia data become extremely relevant due to the growing frequency of its usage.

Currently, research in the field of active protection of multimedia data (images, video and audio files) focuses mainly on digital watermarking, since it is one of the most effective and efficient ways to prove the authenticity of data and the legitimacy of their owners.

The watermark embedding process consists in modification of the data in such a way as to make the introduced distortions acceptable in terms of accuracy. Methods of digital watermarking can be classified according to the resistance of the carried watermark to modifications of the protected data, or to malicious attacks. Robust watermarking is aimed at solving the problem of copyright protection. For the protection of data authenticity and integrity, semi-fragile and fragile watermarking techniques are used.

The existing copyright protection methods have a number of drawbacks. Many of them require the source data during extraction (such methods are called non-blind). Moreover, they do not always provide a sufficient balance between robustness and fidelity (i.e. visual imperceptibility). Therefore, the development of new methods for multimedia protection is still an urgent task.

II. RELATED WORK

As a rule, image watermarking techniques are distinguished according to the domain into which the protective information is embedded.

In the spatial domain, the watermark information is introduced into the carrier image by the direct change of the pixel values [1-3]. The main advantage of these methods is low computational complexity.

In the transform domain, embedding is performed via the transition to the decomposition matrix of the image and the alteration of its coefficients [4-10]. Such a transition is realized using known transformations (Fourier, cosine, wavelet, etc.), or their combinations. The most common approach to robust watermarking is a combination of discrete wavelet transform and singular value decomposition.

The transform domain methods demonstrate high robustness against carrier modifications, and at the same time provide good fidelity, but on the other hand, the computational cost of their implementation is considerable.

The watermark can be specified as a bit sequence or a bitmap image. The second type is most preferable, because even after possible distortions of the carrier image, the watermark can be verified by matching with the original using the correlation analysis. However, such verification can be considered non-accurate in case when the watermark image is significantly damaged.

In [11], the authors proposed a method for image protection based on embedding of robust watermarks constructed in a special manner. The watermarking process does not require a transition to the spectral domain and the extraction procedure is performed without applying correlation analysis. The embedding strategy consists in the summation of the image with a “noise-like” signal serving as a secondary carrier for a bit sequence. The noise-like image is artificially synthesized by arranging the spectral impulses in the spatial-frequency domain and then transitioning to the spatial one using the inverse DFT.

Another variant for construction of noise-like images, proposed in [12], demonstrates significantly higher results of the quality assessment. The main difference of two methods consists in the number of spectral rings: in first method it is equal to the number of bits in the watermark sequence, and in our method it is enough to use only two rings, containing information about the bit value (for example, zero bits are placed on the external ring, and odd bits on the internal one).

In [11] and [12], the noise-like watermarks are embedded according to the additive watermarking strategy, that requires

the presence of the original carrier image during extraction, that is, the above methods are non-blind. In this paper, the additive watermarking is replaced with the least significant bit (LSB) watermarking strategy. As a rule, LSB embedding is not used in robust watermarking because of low resistance to modifications. It is shown that due to the unique features of noise-like watermarks, the robustness of LSB schemes can be significantly increased, which allows to provide the possibility of their application in the task of protection against unauthorized copying and illegal distribution.

III. Proposed Approach

The idea of the proposed method is to construct a noise-like watermark image using a key sequence of bits, serving as verification information during the extraction process.

Embedding of a noise-like signal instead of an ordinary image is more beneficial for two reasons. Firstly, the use of a key sequence for verification allows to unambiguously detect its presence or absence, i.e., makes it possible to avoid inaccuracies arising as a result of classical detection approaches (for example, correlation analysis). Secondly, noise-like images can be reconstructed from a limited set of points, and even significant distortions do not prevent the correct extraction of the sequence. Thus, the use of such images can noticeably increase the information capacity and robustness of classic watermarking schemes.

A. Construction of a Noise-like Watermark

First, a symmetric two-dimensional spectrum is synthesized on the basis of the primary key sequence. In the frequency domain, the delta impulses are located on two circles of different size according to the parity of the watermark bit: “zeros” are placed on the external circle, and “ones” on the internal. All the impulses are arranged with a certain step, except a special synchronization mark, which signals the beginning of the sequence. The values of the impulses are selected randomly: this allows to create different noise-like images for the same watermark sequence.

When the spectrum is formed, a two-dimensional inverse discrete Fourier transform (DFT) is calculated, to obtain the two-dimensional image of a noise-like watermark (Fig. 1).

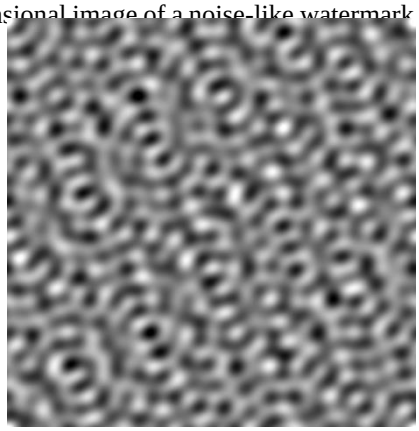

Fig. 1. Noise-like image constructed for $l = 10$, $r = 10$, $\Delta r = 8$.

A detailed description and study of the noise-like image construction is given in [13].

B. Watermark Sequence Restoration

The procedure for watermark sequence restoration begins with the calculation of the two-dimensional spectrum of a noise-like image. For this purpose, a two-dimensional DFT is used.

Next, the resulting spectrum is analyzed, and the spectral components having the largest amplitude (i.e. impulses) are determined.

The detection of amplitude peaks is performed usinglocal filter (here, the size of a local window is 3×3). First, local maxima of the DFT module are selected, and other pixels within the window are assigned zero:

$$|F(n_1,n_2)| = 0,\ if\ |F(n_1,n_2)| < \max_{m_1,m_2} |F(n_1+m_1,n_2+m_2)|$$

where $m_1, m_2 = \overline{-1,1}$, and $n_1, n_2 = \overline{0,N}$. After this, the list of values remaining non-zero is formed, sorted and the greatest $2\times(l+2)$ values are taken for the further processing.

After this, it become possible to examine the presence of an embedded information: the chaotic arrangement indicates the absence of the watermark sequence, but if the impulses are located on two concentric circles, then the procedure of watermark sequence is continued.

At the last step, the synchronization mark is localized, and finally, the key sequence can be unambiguously extracted.

C. Watermark Embedding

The key idea of embedding procedure consists in a simple least significant bit strategy. However, in this paper, watermark bits are embedded only into those regions of the carrier image, that have high variance values. This ensures good properties of watermark imperceptibility. Furthermore, the same watermark pixel is introduced repeatedly into several pixels of the carrier image, which provides robustness against transformations.

The embedding procedure is performed as follows.

1) First the carrier image of size $N \times N$ is divided into blocks of size $m \times m$.

2) For each block, the variance D is calculated.

3) The blocks with variance values $D > T$ are selected as carrier block (i.e. the watermark bits will be embedded only into blocks with high variance).

4) The watermark image of size $N \times N$ is converted to the range of [0,15], so the values of pixel brightness are represented by 4-bit numbers.

5) After this, the watermark image is also divided into blocks of size $m \times m$.

6) The blocks corresponding to carrier blocks with high variance are selected.

7) Within each watermark block, one pixel is chosen for embedding. It is preferable to select middle pixel.

8) The selected watermark pixel is embedded into each pixel of the corresponding carrier block by altering the four least significant bits.

D. Watermark Extraction

When extraction, the following procedure is performed.

1) First, the watermarked image is divided into blocks and the blocks of high variance are determined.

2) For each found block, the four least significant bits are extracted from each pixel.

3) The extracted values are averaged to obtain only one watermark pixel value for each block.

4) For recording the extracted watermark values, a blank raster grid of size $N \times N$ is created and divided into blocks.

5) In case if the corresponding block of the watermark image carries the watermark pixel, the extracted value is put into the center of the watermark block.

Due to the features of the embedding procedure, the watermarked image carries only few watermark pixels. So, it turns out that some watermark pixels remain empty after the extraction procedure. Therefore, the watermark image is restored using the Nearest Neighbor interpolation method.

IV. Experimental Study

To evaluate the efficiency of the proposed method, the experimental study on its quality was conducted. The test images are taken from the Waterloo Grayscale Set [14]. The watermark dataset comprises 100 noise-like images produced for parameters $l = 10, r = 10, \Delta r = 8$. The sizes of both carrier and watermark images are $N \times N = 512 \times 512$.

A. Embedding Quality

To evaluate the visual imperceptibility, the peak signal-to-noise ratio (PSNR) is calculated. In the following experiment, the variance threshold T is a variable parameter. The results are shown in Fig.2. The figure provides the average value calculated after embedding of 100 watermarks into each image.

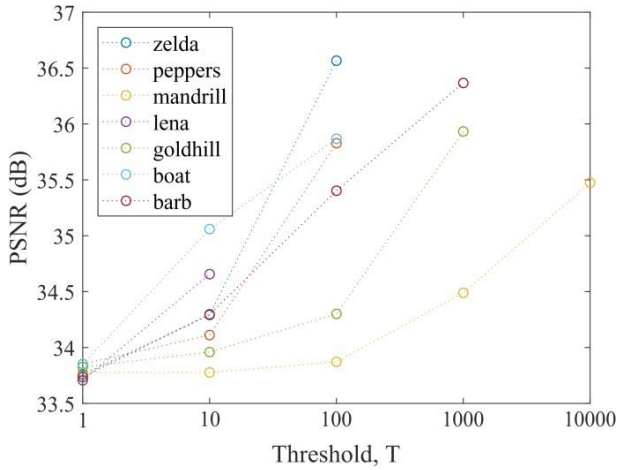

Fig. 2. Dependence of PSNR on the parameter T.

It should be noted that, in some cases, not all the watermarks were extracted correctly. So, the corresponding points on the graphics are absent. This can be explained by the fact that for particular images, growth of T significantly decreases the number of blocks for embedding, and thus the number of watermark pixels, extracted from this image, is not enough for correct restoration of the noise-like watermark. The number of blocks used for embedding into each image depending on the T value is shown in Fig. 3.

It can be seen from Fig. 2, that the values of PSNR are growing with the increase of the threshold T. But, as already mentioned, this value is limited from above. So, the value of T should be selected manually depending on the statistical properties of the carrier image.

The influence of the variance threshold on robustness properties of the proposed watermarking scheme is discussed in the next Subsection.

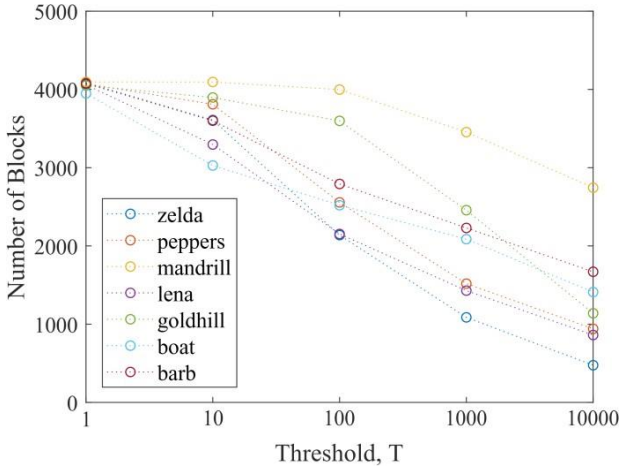

Fig. 3. Number of carrier blocks depending on image variance.

B. Robustness

The task of copyright protection requires robustness against various attacks aimed at watermark removal. This section comprises several computational experiments for evaluation of method resistance to malicious modifications.

The presented results reflect the dependence of the watermark robustness on a variable threshold value T. For each type of distortion, the following procedure was performed. 100 noise-like watermarks were successively embedded into a carrier image. Each time the watermarked image was subjected to distortion of a given degree. If at least 98 of 100 watermarks were extracted with no errors, the distortion is considered acceptable. Each table shows the maximum allowable distortion, which does not affect the probability of correct extraction.

According to the results of the previous experiment, in some cases, the watermark extraction is impossible due to the low carrier capacity. Obviously, these cases are not considered, and denoted with "-". The case of T = 1 is also excluded from investigation because of low PSNR results (see Fig. 2).

Table I shows the maximum allowable size of local window (in pixels) when median filtering.

TABLE I. Robustness against median filtering

Image	Embedding Parameter		
	***T* = 10**	***T* = 100**	***T* = 1000**
zelda	17	7	-
peppers	19	11	-
mandrill	21	21	17
lena	13	-	-
goldhill	17	17	11
boat	9	7	-
barb	17	11	7

Table II shows the maximum allowable share of "salt-and-paper" noise added.

TABLE II. ROBUSTNESS AGAINST NOISE ADDITION

Image	Embedding Parameter		
	T = 10	*T = 100*	*T = 1000*
zelda	0.85	0.45	-
peppers	0.85	0.7	-
mandrill	0.85	0.85	0.8
lena	0.8	-	-
goldhill	0.8	0.8	0.7
boat	0.75	0.45	-
barb	0.8	0.75	0.5

Table III shows the minimum allowable quality factor (*QF*) when JPEG compression. In this experiment, the low *QF* values correspond to the high values of compression ratio. The highest possible quality factor is 100, which corresponds to lossless compression.

TABLE III. ROBUSTNESS AGAINST COMPRESSION

Image	Embedding Parameter		
	T = 10	*T = 100*	*T = 1000*
zelda	25	90	-
peppers	35	80	-
mandrill	80	80	85
lena	50	-	-
goldhill	65	75	90
boat	85	90	-
barb	55	85	95

Table IV shows the maximum allowable size of the cropped fragment, represented via cropping coefficient

$$k_{cr} = 1 - \frac{N_{cr} \times N_{cr}}{N \times N}.$$

TABLE IV. ROBUSTNESS AGAINST CROPPING

Image	Embedding Parameter		
	T = 10	*T = 100*	*T = 1000*
zelda	0.4	0.2	-
peppers	0.4	0.2	-
mandrill	0.4	0.4	0.3
lena	0.4	-	-
goldhill	0.4	0.4	0.1
boat	0.1	-	-
barb	0.4	0.1	-

Table V shows the maximum allowable size of the tampered fragment, represented via coefficient $k_{tamp} = \frac{N_{tamp} \times N_{tamp}}{N \times N}$. The tampering attack is performed by setting at random the pixel values of a chosen fragment.

TABLE V. ROBUSTNESS AGAINST FRAGMENT TAMPERING

Image	Embedding Parameter		
	T = 10	*T = 100*	*T = 1000*
zelda	0.65	0.1	-
peppers	0.65	0.5	-
mandrill	0.65	0.65	0.6
lena	0.55	-	-
goldhill	0.65	0.55	0.4
boat	0.5	0.1	-
barb	0.65	0.5	0.2

According to the obtained results, the proposed method of LSB-embedding combined with the use of noise-like images, provides good robustness properties. Thus, the watermark can still be detected after median filtering (for window size of up to 21×21), noise addition (for up to 85 percent occupancy), compression with low quality factor (for *QF* of up to 25), cropping (for the size of up to 40%), and fragment tampering (for the size of up to 65%).

V. CONCLUSION

In this paper, the method for construction of highly-robust digital watermarks is proposed. The so-called noise- like watermarks are synthesized artificially using a key sequence, serving as verification information during the extraction process. The main goal of the research is to investigate the possibility of the method application for the protection of raster images against illegal distribution.

The constructed watermarks are embedded into bitmap images using the least significant bit (LSB) strategy. It is shown that, due to the unique features of the noise-like watermarks, the robustness of LSB schemes can be significantly increased, which allows to provide the possibility of their application in the task of protection against illegal distribution.

The results of the conducted experiments demonstrate clear advantages of the proposed watermarking method over existing analogues: the noise-like watermark images possess high robustness against carrier modifications and malicious attacks, while the embedding into the spatial domain does not significantly decrease the carrier quality.

REFERENCES

[1] M. Sadeghi, R. Toosi and M. A. Akhaee, "Blind gain invariant image watermarking using random projection approach," Signal Processing, vol. 163, pp. 213-224, 2019.

[2] R. Toosi, M. Sadeghi and M. A. Akhaee, "Robust image watermarking using sample area quantization," Multimedia Tools and Applications, vol. 78, no. 5, pp. 34963-34980, 2019.

[3] A. Jobin and P. Varghese, "An imperceptible spatial domain color image watermarking scheme," Journal of King Saud University - Computer and Information Sciences, vol. 31, pp. 125-133, 2019.

[4] H. S. Devi and K. M. Singh, "Red-cyan anaglyph image watermarking using DWT, Hadamard transform and singular value

decomposition for copyright protection," Journal of Information Security and Applications, vol. 50, no. 102424, pp. 1-7, 2020.

[5] K. Madhavi, G. Rajesh and K. S. Priya, "A Secure and Robust Digital Image Watermarking Techniques," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 12, pp. 2758-2761, 2019.

[6] S. Sharma, H. Sharma and J. B. Sharma, "A gradient method for design of multiorder varied-depth binary diffraction gratings – a comparison," Applied Soft Computing Journal, vol. 84, no. 105696, pp. 1-18, 2019.

[7] R. Noor, A. Khan, A. Sarfaraz, Z. Mehmood and A. M. Cheema, "Highly robust hybrid image watermarking approach using Tchebichef transform with secured PCA and CAT encryption," Soft Computing, pp. 1-9, 2019.

[8] S. P. Singh and G. Bhatnagar, "A Robust Watermarking Scheme for Copyright Protection," Proceedings of 3rd International Conference on Computer Vision and Image Processing, vol. 2, pp. 431-443, 2018.

[9] C. Wang and X. Zhou, "A Robust Color Image Watermarking Algorithm Based on APDCBT and SSVD," Symmetry, vol. 11, no. 1227, pp. 1-18, 2019.

[10] H. J. Ko, C. T. Huang, G. Horng and S. J. Wang, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation," Information Sciences, pp. 1-33, 2019.

[11] N. I. Glumov and V. A. Mitekin, "The new blockwise algorithm for large-scale images robust watermarking," Computer Optics, vol. 35, no. 3, pp. 368-372, 2010.

[12] Y. Vybornova, "Method for Image Copyright Protection Based on Construction of Highly Robust Watermarks," IEEE 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-4, 2020.

[13] Y. D. Vybornova and V. V. Sergeev, "New method for GIS vector data protection based on the use of secondary watermark," Computer Optics, vol 43, no. 3, pp. 474-483, 2019. DOI: 10.18287/2412-6179-2019-43-3-474-483.

[14] Greyscale Set 2. The Waterloo Fractal Coding and Analysis Group: Image Repository, 2009 [Online]. URL: http://links.uwaterloo.ca/Repository.html.