I J C T A, 9(40), 2016, pp. 607-613 ISSN: 0974-5572

A Robust Secure Zero Watermarking for Digital Videos in Slantlet Domain

Ayesha Shaik* and V. Masilamani*

ABSTRACT

Recently, the research in digital communication has been advanced rapidly. It has made the multimedia communication easier and efficient, where the digital data can be copied or sent without degradation in the quality of the data. But the attackers are misusing the advancements in the technologies, which is creating a great trouble for the copyright holders of the data. In order to protect the copyrights of the data owners, digital watermarking technologies are being very helpful. But in traditional watermarking schemes, copyrights or information of owners needs to be embedded in the data which will degrade the quality of the data.So, a zero watermarking scheme is proposed in this article in Slantlet domain for video, where the zero watermark is generated from the Slantlet coefficients characteristics without disturbing the original data. The proposed scheme has been tested on the standard data set. The technique is analyzed experimentally and it is shown robust to a set of attacks such as Gaussian and salt & pepper noise, low pass filtering, median filtering, mean filtering, frame dropping, frame averaging and requantization.

Keywords: Watermarking, zero watermark, robust, Slantlet, bit error rate, Video, Secure

1. INTRODUCTION

In recent years, the scientific and technical advances in research for effective and efficient multimedia communication has been improved drastically. This has affected the digital communication not only in a positive manner, but also in a negative manner. The authentication of the digital data owner has been troubled because of the effective communication of the digital data which helps to generate the multiple duplicate copies of the digital data with the similar quality of the original data. In order to protect the copyrights of the owner, digital watermarking technique is used as one of the favorable options. In this technique, a copyright of the owner is inserted into the digital data for ownership authentication. Other applications of digital watermarking are data authentication, user authentication, broadcast monitoring, etc. Digital watermarking can be classified based on the (i) embedding domain: spatial, transform and dual (both spatial and transform)(ii) transparency of the watermark: visible and invisible, (iii) tolerance of the watermark: robust, semi-fragile and fragile and (iv) embedding method: additive and multiplicative [1-4].

In digital watermarking, a copyright or a logo (information of the owner) is embedded directly into the original data which will bring a slight perceptual degradation in the watermarked data. Ideally, there should not be any perceptual difference between the original and watermarked data, i.e, imperceptibility. But for copyright protection, we need to embed the information in such a way that it is robust to attacks. In order to trade-off between imperceptibility and robustness HVS (human visual system) are used [5-7]. Researchers have developed a technique in which copyrights can be protected without embedding any information of the owner. This technique is known as zero watermarking scheme, where no watermark is embedded but the watermark is generated from the characteristics or the properties of the original data. Zero watermarking schemes have become popular because we can authenticate the ownership without embedding the watermark.

* Department of Computer Engineering, Indian Institute of Information Technology Design and Manufacturing, Kanchepuram, Tamilnadu, India, *Emails: ayeshanoormd@gmail.com, masila@iiitdm.ac.in*

The zero watermarking techniques for audio samples have been discussed in [8-15]. A zero watermarking with spatial domain based neural network is discussed in [13]. In [14], DWT with chaotic modulation has been used for zero watermarking. Using LPCC (Linear Prediction Cepstrum Coefficients), a robust zero watermarking scheme for audio is discussed in [16]. In [17], an audio zero watermarking scheme byenergy comparison is presented.

The transform domain zero watermarking for audio using discrete wavelet and discrete cosine coefficients is discussed in [18]. A video zero-watermark algorithm based on the Contourlet transform is discussed in [19] for video. Here, the zero-watermark is constructed from the selected key frames which have highest entropy. A video zero-watermarking algorithm based on LPM using DWT and DCT log-polar coordinates is presented in [22]. This technique is resistant to noise, rotation, filtering and compression. A video zero-watermarking algorithm based on text detection is discussed in [20]. A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations is discussed in [21].

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Section IV presents conclusion.

2. PROPOSED ALGORITHM

2.1. Watermark embedding algorithm

A zero watermarking scheme for video is proposed in this article.The zero watermarking technique will not embed any watermark unlike traditional watermarking algorithm, but it will meet the requirements of watermarking scheme such as copyright protection, etc. In this method a zero watermark is generated based on the Slantlet coefficients of the selected FOI (frames of interest) from the detected scenes. Slantlet transform is an equivalent representation to DWT [23]. It provides a better time localization and smoothness.

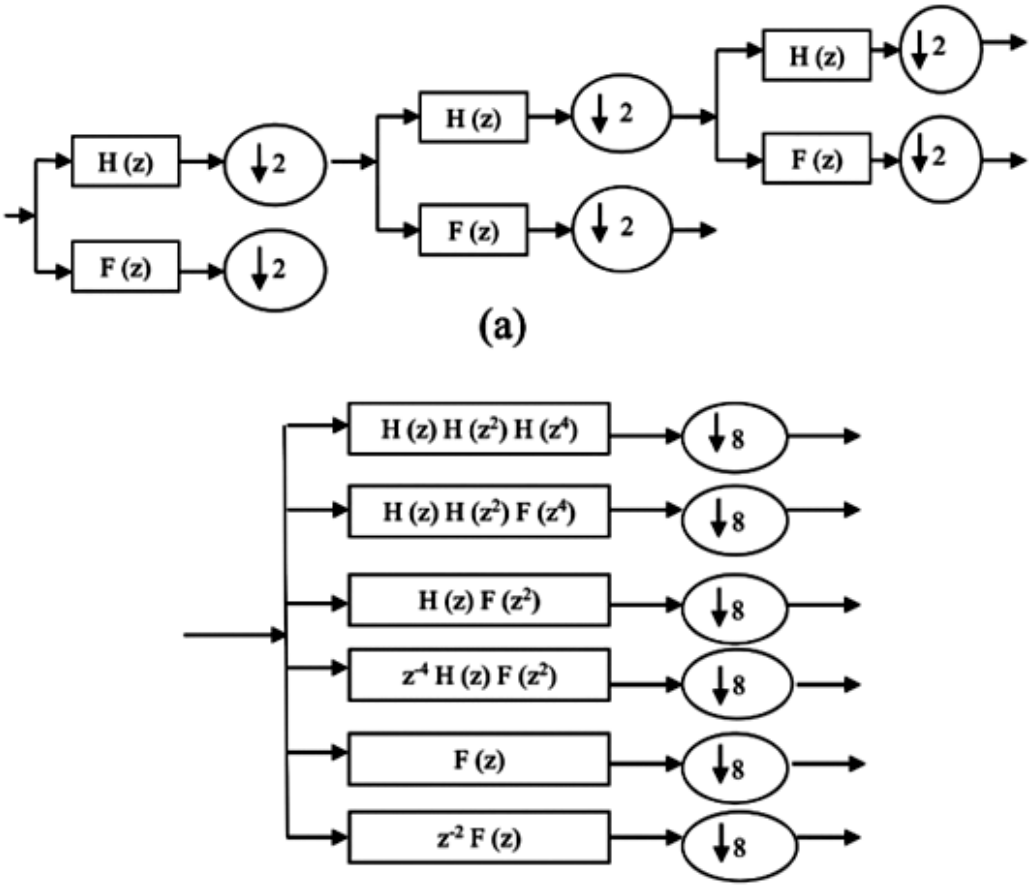

Figure 1: 3-scale filter banks (a) DWT (b) Equivalent Slantlet representation

In the proposed technique, scene detection algorithm is performed on the original video. The scenes are detected based on the absolute histogram differences of the frames. If the difference is more than a predefined threshold, then those framesare detected as scenes in the video. Using this concept all the frames that have more histogram difference are considered as scenes.

$$D_i = \sum_i^N \left| H_i - H_{i+1} \right| \tag{1}$$

Where N denotes number of bins in the histogram and H_i and H_{i+1} are the histograms of i^{th} and $i + 1^{th}$ frames in the video.

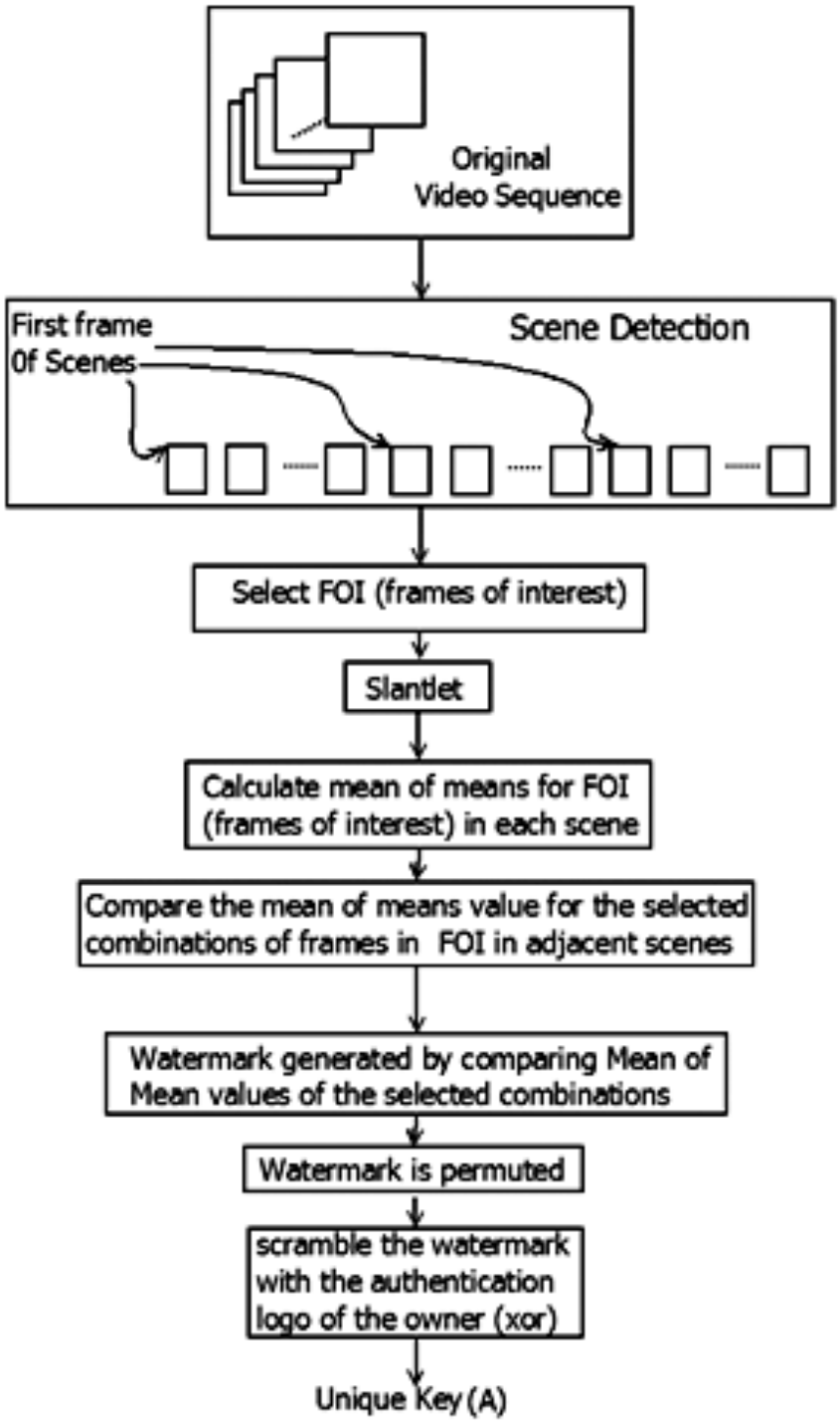

Figure 2: Proposed zero watermarking algorithmblock diagram

Let video sequence, V = (f_{scene_i}), where f_{scene_i} is i^{th} scene in the video. $f_{scene_i} = \left(f^1_{scene_i}, f^2_{scene_i}, f^3_{scene_i}, ..., f^{N_i}_{scene_i}\right)$, where $f^j_{scene_i}$ is the j^{th} frame of $scene_i$ $1 \le i \le S$, where S is the number of scenes in the video and N_i is the number of frames in $scene_i$. Now FOI (frames of interest) are selected from each ,

$$FOI_{scene_i} = \left\{ f^{10*r+1} scene_i \,/\, r is non-negative integer, 1 \le (10*r+1) \le N_i \right\}.$$

Let us denote frames of interest as

$$FOI_{scene_i} = \left(FOI^1_{scene_i}, FOI^2_{scene_i}, ..., FOI^{K_i}_{scene_i}\right), \text{ where } K_i \text{ is the size of } FOI_{scene_i}.$$

The Slantlet transform coefficients are denoted as

$$T_{i,j} = Slantlet\left(FOI^j_{scene_i}\right), 1 \le j \le K_i$$

Let us compute Mean-of-Means for $T_{i,j}$ as

$$MoM\left(a\right)_j = \sum_{j=a}^{\left\lceil \frac{K_i}{2} \right\rceil} Mean\left(T_{i,j}\right), 1 \le a \le \frac{K_i}{2}.$$

For $1 \le i \le S$ *and* $1 \le a \le \frac{K_i}{2}$,

$$If\ MoM(a)_i > Mom(a)_{i+1} \text{ then}$$
$$w(i, a) = 1 \text{ else } w(i, a) = 0$$

Then linearize w by row-wise concatenation obtaining a linearized zero watermark W. So, now a watermark, W of size $(S-1) * r$ is generated. In order to make this watermark secure, it will be permuted by a secure key and then scrambled by the logo of the owner, A unique to the owner of the original data (for XOR operation linearized watermark W can be reshaped to be 2D). The output will be the scrambled and permuted zero watermark, K.

$$K = P\left(W\right) \oplus A$$

Where $P(.)$ is the permuted operation and $\oplus$ is scrambling or XOR operation. The block diagram for zero watermark extraction is shown in Figure 3.

2.2. Watermark Extraction algorithm

The extraction algorithm process is the similar process to the zero watermark embedding with slight modification after zero watermark generation. After generating the zero watermark from the watermarked image, it is inverse permuted and scrambled with the K as shown.

$$A' = P\left(W'\right) \oplus K$$

Where W' is zero watermark extracted from the possibly modified watermarked image. Then check whether A and A' are equal, if its equal, then the owner is authenticated otherwise it is not authenticated. The block diagram for zero watermark extraction is shown in Figure 4. If there is no modification, then the extracted zero watermark, W' will be exactly equal to W. In this case, A and A' will be exactly equal.

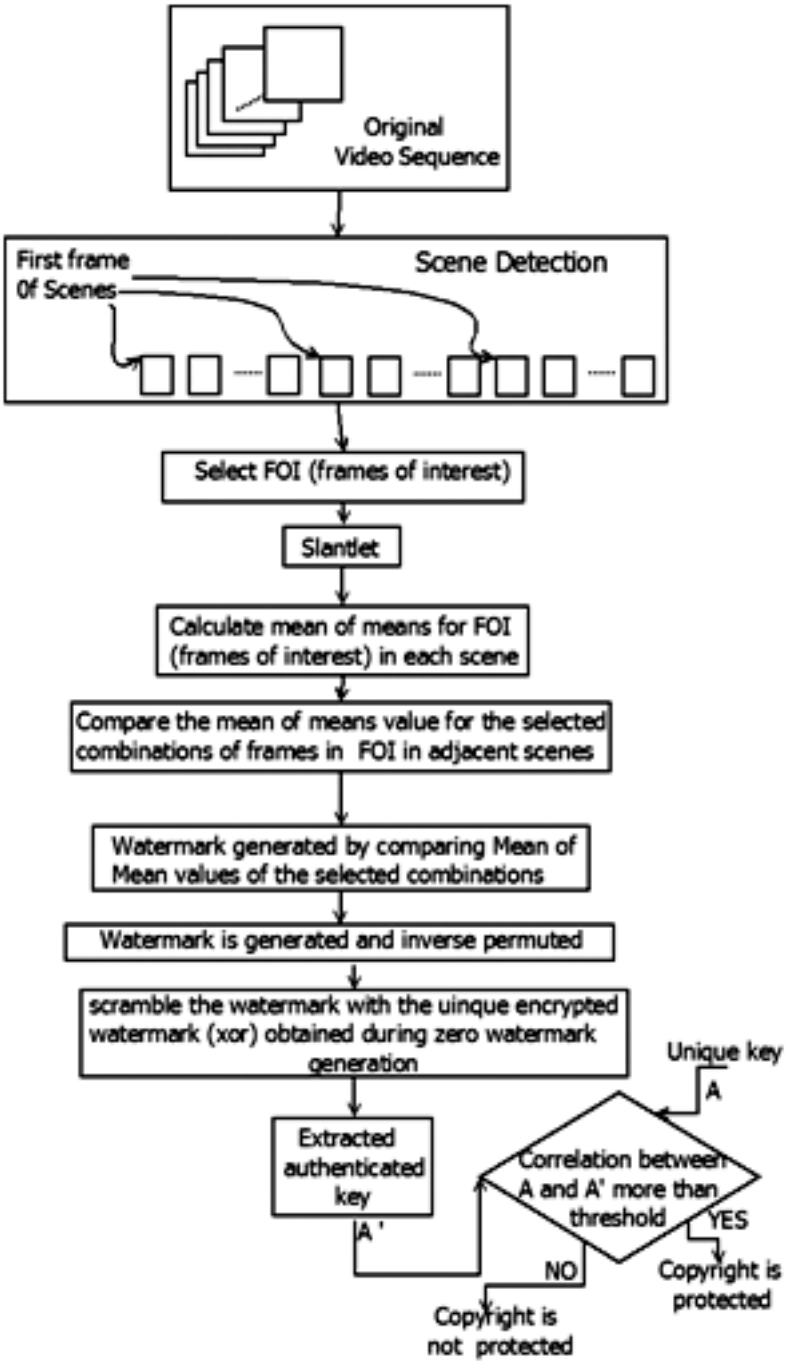

Figure 3: Watermark Extraction algorithm Block Diagram

3. EXPERIMENT AND RESULT

The test video for this experiment has been selected from the VIRAT dataset. The proposed scheme is analyzed with a set of attacks and is shown robust towards a list of attacks tabularized in Table-1. It has been compared with the zero watermarking technique given in [18] in 2D DWT and DCT domain.

Table 1 shows thatthe proposed scheme is more robust to Gaussian, salt & pepper noise, median and mean filtering, quantization, low pass filtering, frame dropping and frame averaging attacks than the method given in [18]. The proposed technique is more robust as only the significant information in video, which are scenes and their successive frames are selectively taken into account for generating zero watermark.

Table 1
Experiment Result

Attack	Proposed Method (Key image)	Proposed Method (Extracted key image)	Bit error rate between the key image and extracted key image	Correlation between the key image and extracted key image	Method given in [13] (Extracted key image)	Bit error rate For method given in [13]	Correlation For method given in [13]
No Attack			0	1		0	1
Gaussian Noise			0.02	0.9877		0	1
Requantization			0	1		0.00	0.9759
Median filtering Size 3 x 3			0	1		0.0092	0.9038
Median filtering Size 5 x 5			0	1		0	1
Median filtering 7 x 7			0	1		0.148	0.8539
Average filtering size3 x 3			0	1		0.0352	0.9257
Average filtering With window size5 x 5			0	1		0.0644	0.883
Average filtering With window size7 x 7			0	1		0.0712	0.8484
Salt & Pepper noise			0	1		0.001d	0.99dd
Low pass filtering			0	1		0	1
Frame dropping			0	1		0.0dd4	0.9d10
Frame averaging			0	1		0.0144	0.9d9d

4. CONCLUSION

In this article, a zero watermarking scheme for video has been proposed in Slantlet domain. The zero watermarking schemes are gaining a lot of interest now a days, because without disturbing the original data, we can protect the copyrights of the owner. In the zero watermarking schemes the watermark is not embedded, but a zero watermark is generated from the characteristics of the original data. In the proposed technique, the watermark is generated from the mean properties of the Slantlet coefficients of the detected scenes. To make the zero watermark secure, it has been permuted and then scrambled by the unique authentication key of the owner. The proposed technique has been implemented on a Foreman, Container, Football videos in standard video database and is showed robust to a list of attacks such as Gaussian, salt & pepper noise, median and mean filtering, quantization, additive white Gaussian noise, low pass filtering, frame dropping and frame averaging attacks.

REFERENCES

[1] Sadreazami, H., M. Omair Ahmad, and M. N. S. Swamy, A Robust Multiplicative Watermark Detector for Color Images in Sparse Domain." IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 62, no. 12 pp. 1159-1163, 2015.

[2] Sadreazami, H., M. Omair Ahmad, and M. N. S. Swamy. "Optimum multiplicative watermark detector in contourlet domain using the normal inverse Gaussian distribution." In 2015 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1050-1053. IEEE, 2015.

[3] Sadreazami, Hamidreza, M. Omair Ahmad, and M. N. S. Swamy. "Multiplicative Watermark Decoder in Contourlet Domain Using the Normal Inverse Gaussian Distribution." IEEE Transactions on Multimedia, vol. 18, no. 2, pp. 196-207, 2016.

[4] Sadreazami, Hamidreza, M. Omair Ahmad, and MN Shanmukha Swamy. "A study of multiplicative watermark detection in the contourlet domain using alpha-stable distributions." IEEE Transactions on Image Processing, vol. 23, no. 10, pp. 4348-4360, 2014.

[5] B. Chen and G. W. Wornell "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding" IEEE Trans. Inf. Theory., vol. 47, no. 4, pp. 1423-1443, 2001

[6] B. C. Mohan and S. S. Kumar "Robust digital watermarking scheme using contourlet transform" Int. J. Comput. Sci. Netw. Security, vol. 8, no. 2, pp. 43-51, 2008

[7] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris "A medical image watermarking scheme based on wavelet transform" Proc. 25th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., pp. 856-859,

[8] T. Sun, W. Quan, and S.-X. Wang, "Zero-watermark watermarking for image authentication," in Proceedings of the Signal and Image Processing, Kauai, Hawaii, USA, pp. 503–508, August 2002.

[9] G. Horng, C. Chen, B. Ceng, and T. Chen, "Neural network based robust lossless copyright protection technique," http://www.csie.cyut.edu.tw/ TAAI2002/TAAI2002PDF/Parallel

[10] L. Ghouti, A. Bouridane, M.K. Ibrahim, and S. Boussakta,"Digital image watermarking using balancedmultiwavelets", *IEEE Trans. Signal Process*., 2006, Vol.54, No. 4, pp. 1519-1536.

[11] Q. Wen, T.-F. Sun, and S.-X. Wang, "Concept and application of zero-watermark," Tien Tzu Hsueh Pao/Acta Electronica Sinica, vol. 31, no. 2, pp. 214–216, 2003.

[12] S. Yang, C. Li, F. Sun, and Y. Sun, "Study on the method of image non-watermark in DWT domain," Chinese Journal Image Graphics, vol. 8A, no. 6, pp. 664–669, 2003.

[13] J. Sang, X. Liao, andM. S. Alam, "Neural network based zero-watermark scheme for digital images," Optical Engineering, vol. 45, no. 9, 2006.

[14] C. Hanqiang, X. Hua, L. Xutao, L. Miao, Y. Sheng, and W. Fang, "A zero-watermarking algorithm based on DWT and chaotic modulation," in Proceedings of SPIE Independent Component Analyses, vol. 6247, pp. 1–9, Orlando, Fla, USA, 2006.

[15] L. Jing and F. Liu, "Double zero-watermarks scheme utilizing scale invariant feature transform and log-polar mapping," in Proc. of the IEEE International Conference on Multimedia and Expo, pp. 2118–2121, Las Vegas, Nev, USA, February 2007.

[16] S. M. Tsai, A Robust Zero-Watermarking Algorithm for Audio Based on LPCC, IEEE Conference on International Conference on Orange Technologies (ICOT), pp.63-66, 2013.

[17] Yang Yu, Lei Min, Cheng Mingzhi, Liu Bohuai,Lin Guoyuan, Xiao Da. An Audio Zero-WatermarkScheme Based on Energy comparing. ChinaCommunications, 2014, vol 11, no. 7, pp. 110-116, 2014.

[18] Yu, Yang, Min Lei, Xiaoming Liu, Zhiguo Qu, and Cheng Wang. "Novel zero-watermarking scheme based on DWT-DCT." China Communications, vol. 13, no. 7, pp. 122-126, 2016

[19] Xuesong, Chen, Bu Guanglong, Li Haotian, and Bi Hongbo. "A Video Zero-watermark Algorithm Based on the Contourlet Transform." In 3rd International Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013.

[20] Xu, Qishuai, Jianfeng Lu, Xinxin Peng, Shijie Yuan, and Li Li. "A video zero-watermarking algorithm based on text detection." In Proc. of the IEEE 16th International Conference on Communication Technology (ICCT), pp. 328-333, 2015.

[21] Khan, Aihab, and Syed Afaq Husain. "A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations." The Scientific World Journal, 2013.

[22] Qiao, Luyan, and Jongweon Kim. "A video zero-watermarking algorithm based on LPM." Multimedia Tools and Applications, pp. 1-14, 2015.

[23] Ansari, Irshad Ahmad, Millie Pant, and Chang Wook Ahn. "Artificial bee colony optimized robust-reversible image watermarking." Multimedia Tools and Applications, pp. 1-25, 2016.