A New Watermarking Method for Video Authentication with Tamper Localization

Yuliya Vybornova(✉)

Samara National Research University, Samara, Russia
vybornovamail@gmail.com

Abstract. In this paper, a new method for video authentication is proposed. The method is based on construction of watermark images, which serve as a secondary carrier for the binary sequence. A unique watermark image is embedded into the coefficients of Discrete Wavelet Transform of each video frame. The analysis of images extracted from video allows to detect spatial attacks, and the sequence carried by the extracted images provides the ability to determine the type of temporal attack and localize the frames, which are tampered. The experimental study on the method quality and efficiency is conducted. According to the results of experiments, the method is suitable for solving authentication tasks. Furthermore, the method is robust to compression and format re-encoding.

Keywords: Digital watermarking · Authentication · Video protection · Tamper localization · Forgery detection · Forensics · Discrete Wavelet Transform · MPEG-4 · Motion JPEG

1 Introduction

Today, the number of tasks requiring video content authentication is growing steadily. The ability to prove the video authenticity is especially important when it is used as evidence of human actions, for example, in court. In most cases, it is difficult to guarantee that the digital video obtained as evidence is exactly the one that was actually captured by the camera.

The video authentication system ensures the integrity of digital video and checks, whether the video is tampered or not. But in most cases, such systems do not provide the information about the type of attack, and video is just considered inapplicable as evidence. A video can be modified by replication, deletion, insertion and replacement of frames or objects in frames. Thus, the two common types of video tampering attacks are spatial (i.e. modification of frame content) and temporal (i.e. modification of frame order).

The authentication of digital video can be performed both by means of cryptography, such as digital signatures and hash functions, and by means of watermarking. Such methods belong to the class of active protection, that is, protective measures are performed before attempting an attack.

L. J. Chmielewski et al. (Eds.): ICCVG 2020, LNCS 12334, pp. 201–213, 2020.
https://doi.org/10.1007/978-3-030-59006-2_18

In most cases, the cryptographic primitives only provide data integrity verification without the ability to localize the tampered fragment. For example, in [1] hash is calculated using Discrete Cosine Transform and Singular Value Decomposition. In [2] a blockchain model is proposed, which uses both hashes and signatures to verify the video integrity. However, some methods like proposed in [3] do provide the ability of tamper localization. The authors propose to form hashes robust to temporal attacks but allowing to localize the tampered content of the video frame.

Another direction of forgery detection is represented by methods of passive protection, which can determine the fact of malicious modifications by analyzing the statistical properties of the data. These methods are typically implemented via machine learning tools. Generally, the efficiency of such methods depends on the particular task, video content, and codecs used for compression. In addition, most existing methods are very sensitive to camera settings and lighting conditions [4].

Thus, the task of this research is to create a universal method that allows to determine and localize both temporary and spatial attacks, and at the same time does not depend on video content and format. Semi-fragile digital watermarking seems to be the best solution since it allows to avoid disadvantages mentioned above for other techniques.

The rest of the paper is organized as follows. Section 2 overviews the related work. In Sect. 3, the proposed approach for video watermarking is presented. Section 4 comprises experimental study on quality and efficiency of the proposed method. Section 5 provides general conclusions and the main issues of the future work.

2 Related Work

The main idea of most existing video watermarking methods is to embed the protective information into frames by introducing distortions that are acceptable in terms of accuracy and usually invisible to the legitimate user.

Generally, the watermark is defined by a bit vector of a given length or a bitmap image. In the first case, it is hard to ensure the enough robustness providing the integrity of the embedded bits. In the second case, the embedded image can also be distorted even when legitimate modifications. For this reason, the process of watermark verification requires the calculation of bit error rate (BER) or normal correlation (NC). Such approach to verification is suitable in the task of copyright protection, but when verifying video authenticity, it can be hard to realize whether the concrete values of BER/NC are acceptable, or they should be considered as a confirmation of attack.

The most common classification divides existing watermarking methods into two groups depending on the embedding domain. In the spatial domain, the watermark is embedded into the video frame by directly changing the brightness values of pixels, while in the transform domain, the watermark is introduced by changing the decomposition coefficients of the image matrix. Most research in the field of video watermarking focuses on the second group of methods, i.e. methods of embedding in the transform domain, since they demonstrate high robustness, and at the same time introduce less visible distortion than methods of embedding in the spatial domain. The cost for these advantages is a high computational complexity in comparison with watermarking in the spatial domain.

The discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) are the most commonly used today. DCT is more often used in steganography and less often in watermarking. In [5] DCT is applied in combination with DWT and SVD, and in [6] authors use discrete sine transform instead.

Applying SVD in combination with various transforms is a very spread technique, since it provides a very high robustness of the embedded information. Thus, in [7] SVD is applied to one of DWT sub-bands; and in [8] SVD is applied to the watermark image, which is then embedded into DWT sub-band. In [9] authors propose to use SVD as a domain for the encrypted contourlet coefficients. The main drawback of most methods using SVD is that they require the original video, i.e. they are non-blind. However, there exist some methods allowing to perform extraction from SVD without using the host signal, e.g. [10], but the informational capacity of such methods is much lower compared to non-blind ones.

In video and image watermarking, the most common transform domain is the space of DWT coefficients, since it allows to preserve quality of the watermarked data, as well as provides high watermark capacity and robustness [11].

The most used and the simplest wavelet decomposition is Haar wavelet transform. According to the research provided in [12], the Haar DWT provides the highest quality of the extracted information compared to other wavelet decompositions. As already mentioned above, DWT can be combined with DCT and/or SVD for increasing the watermarking quality [5,7,8]. However, there are a variety of another techniques using DWT. Thus, for example, in [13] authors propose to embed different fragments of a watermark into different scenes of the video, while for motionless frames the same watermark fragments serve as embedding information. In [14] authors proposed to increase robustness by embedding short messages only into the region of interest calculated on the basis of features extracted from the carrier video. The watermark is embedded into various bit planes of 2-level DWT sub-bands.

Furthermore, video watermarking methods can be classified into format-oriented and robust to transcoding. The methods of the first type can be applied only to particular video formats. In recent years, a variety of methods were proposed for MPEG-4 standard. Despite the fact that MP4 format is one of the most known nowadays, the problem of its protection is still actual. In [15] the watermarking process is based on the Chinese Remainder Theorem. The watermark images are hard to verify because of the distortions introduced by the embedding procedure. Thus, the method is not suitable for authentication purposes. In [16] authors proposed a robust to recompression watermarking scheme based on chromatic DCT. The scheme utilizes major features of H.246/AVC coding standard and allows to detect frame tampering. In [17] authentication information is constructed not only on the basis of the video features, but also using the audio content of MP4 file, and then embedded in subtitles. This scheme allows to detect frame addition and removal. In [18] the video hash is encrypted and embedded into audio data, and the encrypted audio hash is embedded into synchronization information of MP4 file. The proposed scheme is robust against compression and can be applied for tamper detection.

Transcoding invariant methods are mostly refer to robust watermarking. For example, the mentioned above methods [8,9], which use SVD, allow to transcode the video into the other formats. In [19] a watermark image of a small size is embedded into a given area of a key frame. In this approach, authentication requires manual selection of parameters, until the watermark becomes clearly visible.

As for authentication tasks, [17] allows to detect temporal attacks, but can be applied only for video with subtitles. In [20] the authors determine the specific frames among the non-motion frames, and then apply 3D-DWT for embedding. The approach is not resistant to temporal attacks, which means it can be used only to detect them, not to localize. Some methods, like [16] provide the detection of spatial attacks, as well as tamper region localization. In [21] authors propose a fragile watermarking scheme using Least Significant Bit (LSB) embedding strategy, which allows to detect and localize changes on the frame.

Thus, the development of a video authentication method for detection and localization of both spatial and temporal attacks, and applicable for common video formats, is still an actual task, which is solved in this paper.

3 Proposed Method

3.1 Watermark Generation

In this paper, two types of watermarks are considered. The first is a watermark sequence represented by a set of unique binary subsequences s_i of a fixed length l. The length L of the whole sequence $S = s_1, s_2, \ldots, s_K$ depends on the number of frames K in the carrier video, and can be calculated as $L = l \times (K \bmod (2^l - 1))$.

The watermark sequence can be produced by a random permutation $(\sigma(b_1), \sigma(b_2), \ldots)$ of all possible templates b_j of length l and taking the first K elements $(\sigma(b_1), \sigma(b_2), \ldots, \sigma(b_K))$. Here, $j = \overline{1, |\mathbf{B}_l|}$ and $|\mathbf{B}_l| = 2^l - 1$ is a size of a set of all b_j of length l (note, that zero-sequence is excluded).

The second watermark type is a noise-like image used as a secondary carrier for a subsequence s_i. The process of noise-like image construction is shown in detail in one of our previous works [22].

To obtain a noise-like image, its two-dimensional spatial spectrum is formed by arranging the bits of the corresponding watermark sequence in the spectral domain. With an equal angle step, two-dimensional impulses are placed on two rings of different radii r and $r + \varDelta r$, i.e. depending on the value of the corresponding bit of the watermark sequence, the impulse is placed on the ring of a smaller or larger radius. Then, using the inverse discrete Fourier transform (DFT), a transition to a two-dimensional image is performed.

However, in this study the above described method is slightly modified by adding some new distinguishing features to improve robustness and security of the sequence carried inside the noise-like image.

To avoid the watermark image tampering by reproducing the sequence of noise-like images there is a possibility to construct different spectrums and, consequently, different watermark images for the same s_i by setting the values of impulses at random both for real and imaginary parts of the spectrum. Such a modification allows to prevent the attempt of the adversary to construct the same sequence of watermark images and embed it into the tampered video.

Figure 1a and Fig. 1b demonstrate the example of two different watermarks constructed for the same sequence $s = (1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$ with parameters $N = 512, r = 10, \Delta r = 8$.

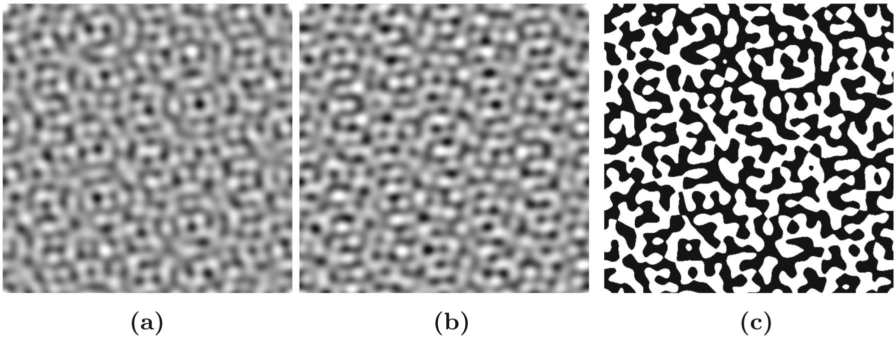


Fig. 1. Noise-like images: (a), (b) halftone; (c) after binarization

The one more change concerns the number of bits per pixel. The method proposed in this paper operates better with binarized noise-like images. This is explained by the fact that video encoding (especially MPEG-4) introduces considerable distortions into the watermark image. So, the binary image is used since it can be restored much more easily than the halftone one. The example of a noise-like image (shown in Fig. 1a) after binarization is shown in Fig. 1c.

3.2 Watermark Embedding

After the construction of the watermark image sequence, each video frame is watermarked by embedding the noise-like image into the wavelet transform domain using LSB-strategy. Such semi-fragile watermarking technique combined with the use of highly robust noise-like watermarks provides robustness against video format change including re-encoding with low compression ratio.

The video V is processed frame-by-frame, and it should be noted that for each frame the watermark image is unique. If the watermark sequence length

$L < K$, then the video should be divided into t blocks of $K_t \leq L$ frames and each frame should be individually watermarked with sequence S.

The use of a unique subsequence s_i for each frame vf_i allows to construct a one-to-one mapping $s_i \leftrightarrow vf_i$ which makes the authentication procedure as easy as possible. By analyzing the extracted sequence and comparing it with the original, the following conclusions regarding the sequence integrity can be made: 1) the absence of the sequence fragment indicates that corresponding frames are dropped; 2) the altered order of s_i is an evidence of frame swapping; 3) repeated s_i is a consequence of frame duplication; 4) zero s_i means that the annular spectrum can not be detected.

Although the binary sequence can be repeated, the sequence of watermark images is unique for each block since the spectrum impulses are randomized at the stage of watermark generation.

The algorithm for watermark embedding is as follows.

1) First, each frame is converted from RGB into YCbCr color space. The Y-component is chosen for the further processing.
2) Next, the location for the watermark is selected, and the Y-component is cropped. The watermark location means an arbitrary $2N \times 2N$ fragment of the video frame. In this paper, the watermark is simply embedded into the center of the video frame (namely, its Y-component).
3) Then, watermark pixels are converted to the range [0; 15], i.e. each pixel is represented by a 4-bit number.
4) After this, frame is converted into wavelet domain using the Haar wavelet transform. The frame is decomposed into four sub-bands of $N \times N$ size: approximation image LL, horizontal detail HL, vertical detail LH, and diagonal detail HH.
5) The watermark pixel values are embedded into the four least significant bits of the chosen sub-band.
6) Next, the inverse DWT is performed.
7) Finally, the initial size of the video frame is restored by adding the cropped fragments of Y-component and combining it with the Cb and Cr chroma components.
8) After transition back to RGB color space, the frames are successively added into resulting video.

3.3 Watermark Extraction

The extraction of watermark image sequence consists in performing of the following steps for each frame.

1) RGB videoframe is converted to YCbCr. The $2N \times 2N$ fragment containing the watermark is selected.
2) The DWT is calculated, and the sub-band used when embedding is selected.
3) The four least significant bits of the sub-band are the 4-bit watermark pixel values.

4) The extracted watermark is converted to the range of [0; 255].
5) The median filter is applied to the watermark image to obtain better results for the further extraction of binary watermark sequence.

To extract the binary sequence carried inside each watermark image, it is necessary to calculate the DFT of the image, to localize the coordinates of the spectral components having a large amplitude (impulses), and to estimate radii of the rings.

To find large spectral impulses, a local window of size 3×3 is used. First, local maxima of DFT module are calculated, and other pixels inside the window are set to zero. Next, the largest $2 \times (l + 2)$ elements are selected from those which remain non-zero.

4 Experimental Study

To evaluate the effectiveness of the proposed method, several computational experiments were conducted. A video dataset contains eight uncompressed videos from MCL-V Database [23]. For each video, the size of frame is 1920×1080 pixels. Number of frames varies from 120 to 180.

The watermark image dataset contains 200 random binarized noise-like images constructed on the basis of a 2000-bit sequence with parameters $l = 10$, $N = 512$, $r = 10$, $\Delta r = 8$.

4.1 Quality and Efficiency

This section provides the experimental study regarding the visual indistinguishability of the embedded watermark and the operability of the proposed method. The experiment is aimed at finding balance between the method efficiency and quality of the watermarked video.

The sequence of watermark images was successively embedded into various DWT sub-bands of each video. The output video was encoded into three most common video formats: .mp4 (MPEG-4), .avi (Motion JPEG AVI), .mj2 (Motion JPEG 2000).

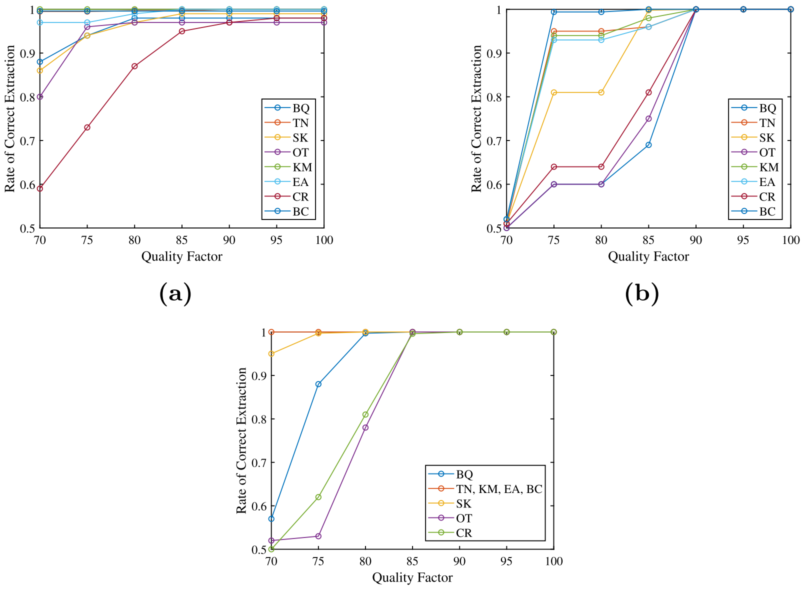
As a measure of the method efficiency, the watermark sequence integrity, is considered. It can be estimated as a rate of its accurate extraction, i.e. a ratio of correctly extracted watermark bits to the total length of the watermark sequence. The rate of correct extraction is denoted by R.

As a measure of fidelity, the common characteristics of the image quality, peak signal-to-noise ratio (PSNR), is calculated.

The experiment has shown that, when embedding into LL sub-band, the watermark becomes visible. HH sub-band demonstrated high imperceptibility, but its robustness to MPEG-4 encoding is a bit lower compared with other detail sub-bands. The best balance between fidelity and efficiency is obtained for HL and LH sub-bands: the results are presented in Table 1.

Table 1. Results of quality assessment

V	HL sub-band						LH sub-band					
	.mj2		.avi		.mp4		.mj2		.avi		.mp4	
	PSNR	R	PSNR	R	PSNR	R	PSNR	R	PSNR	R	PSNR	R
BQ	37.48	1	37.40	1	37.09	0.98	37.40	1	37.31	1	37.04	0.97
TN	36.83	1	36.73	1	34.46	1	36.98	1	36.88	1	34.54	1
SK	37.41	1	37.34	1	35.30	0.99	37.42	1	37.35	1	35.30	0.99
OT	37.29	1	37.19	1	37.08	0.97	37.36	1	37.26	1	37.14	0.97
KM	37.08	1	36.99	1	36.81	1	37.11	1	37.02	1	36.86	1
EA	37.19	1	37.11	1	36.48	1	37.15	1	37.06	1	36.48	0.99
CR	37.53	1	37.44	1	36.01	0.98	37.56	1	37.46	1	36.02	0.99
BC	37.02	1	36.93	1	35.48	0.99	37.04	1	36.95	1	35.49	0.99



(a)

(b)

(c)

Fig. 2. Rate of correct extraction after HL-embedding and encoding with compression: a) MPEG-4; b) Motion JPEG AVI; c) Motion JPEG 2000

4.2 Robustness Against Compression

When evaluating the method robustness, the acceptable (legitimate) modifications should be determined. Since the purpose of this paper is to solve the problem of video authentication, the watermark information should remain unchanged when the video is encoded, as well as re-encoded or compressed.

To show the method invariance to encoding with compression, the following experiment was conducted. The watermark was embedded into video, and then the video was encoded with different quality factor QF. This procedure was performed for three video formats: .mp4, .avi, .mj2.

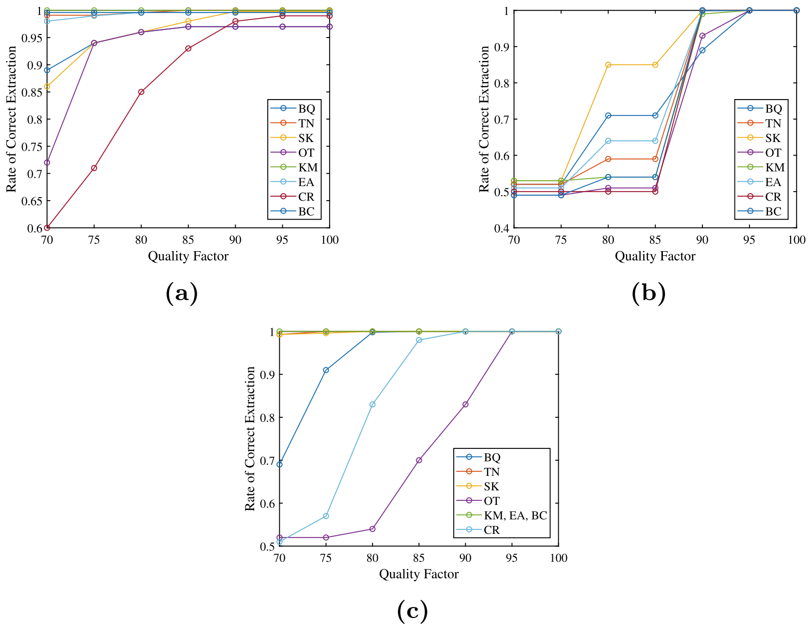


Fig. 3. Rate of correct extraction after LH-embedding and encoding with compression: a) MPEG-4; b) Motion JPEG AVI; c) Motion JPEG 2000

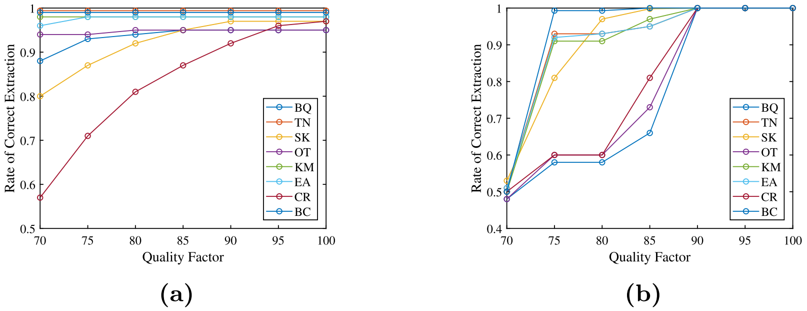
The results of the experimental study for various formats in the case of embedding into HL and LH sub-bands are shown in Fig. 2 and Fig. 3 respectively.

According to the results obtained, the watermark carried in the LH-sub-band is less robust to compression, especially for the case of Motion JPEG AVI encoding. For this reason, the next subsections comprise the results only for embedding into HL sub-band.

4.3 Robustness Against Re-Encoding

It should be noted that when performing an attack, an adversary can re-encode the video with another quality factor. To analyze the possible effect of this manipulation, each video was firstly watermarked and encoded to three different formats, and then re-encoded to the same format with various values of the quality factor.

The results are shown in Fig. 4. It should be noted that for the case of .mj2 format the results coincide with those from Subsect. 4.2. In this regard, the graphics is not provided.



(a)

(b)

Fig. 4. Rate of correct extraction after re-encoding with compression: a) MPEG-4; b) Motion JPEG AVI

Compared with the results obtained for one-time encoding in previous subsection, re-encoding does not significantly affect the extraction rate.

4.4 Temporal Attacks

The experiment comprises three types of temporal attacks: frame removal, frame reordering and frame addition. Before simulating the attacks, the videos from the dataset were watermarked and encoded to MPEG-4 with $QF = 100$. The attacked video was also encoded to MPEG-4 with highest QF value.

1) Frame Removal. The attack was conducted as follows. The video fragments of a given size were removed from the watermarked video. The first frame of the fragment was selected randomly. The size of the removed fragment varied from 10 to 50% of the total number of video frames. To calculate the extraction rate R between extracted watermark sequence and original, the latter was reconstructed by removal of s_i corresponding to deleted frames.
2) Frame Reordering. To conduct this attack, two random video fragments of a given size were swapped. The size of the fragments varied from 10 to 40% of the total size of the video. To calculate the extraction rate R between extracted watermark sequence and original, the latter was reconstructed by changing the order of s_i in correspondence with swapped video fragments.
3) Frame Addition. For this attack, a random video fragment of a given size was copied and inserted into an arbitrary place of the video. The size of the fragments varied from 10 to 50% of the total size of the video. To calculate the extraction rate R, the extracted sequence was reconstructed by removing the sequence fragment extracted from the frames, which were added.

The experiments have shown that authentication quality does not significantly depend on the fraction of changed frames. For this reason, Table 2 provides the results averaged over all cases. According to the results obtained, the watermark sequence is preserved after all types of temporal attacks.

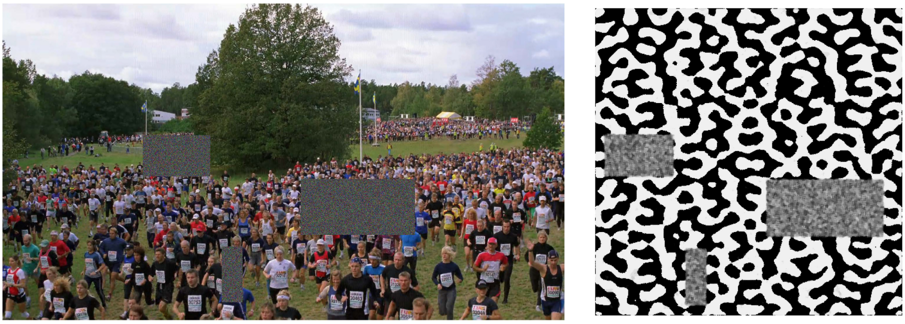
Table 2. Extraction rate after temporal attacks

V	BQ	TN	SK	OT	KM	EA	CR	BC
Deletion	0.95	0.99	0.97	0.96	0.98	0.98	0.97	0.99
Reordering	0.96	0.99	0.97	0.96	0.99	0.99	0.96	0.99
Addition	0.96	0.99	0.98	0.96	0.98	0.98	0.97	0.99

4.5 Spatial Attacks

Besides temporal attacks, the proposed method also allows to detect and localize the spatial attacks, i.e. forgery of video frame content. But, here, instead of the binary sequence, the watermark image itself is used to detect forgery.

To demonstrate the idea, the following experiment was conducted. An arbitrary fragment of the video frame was modified by assigning the pixels with random values. After this, the watermark was extracted from the frame. The "tampered" frame is shown in Fig. 5a, while Fig. 5b shows the watermark extracted from the modified frame.



(a) **(b)**

Fig. 5. a) Tampered frame of CR video; b) watermark extracted from the tampered frame

It can be clearly seen from the Fig. 5, that the distorted fragment of the watermark coincides with the tampered region of the frame.

However, it should be noted that, forgery detection is possible only for the part of the frame, which carries a watermark. In this study, a watermark was embedded into the central part of a video frame, but generally, any fragment (or several fragments) can be chosen depending on the video content.

5 Conclusions and Future Work

In this paper, a new method for video authentication is proposed. The method is based on construction of watermark images, which serve as a secondary carrier for the binary sequence. A unique watermark image is embedded into the coefficients of Discrete Wavelet Transform of each video frame.

The analysis of images extracted from video allows to detect spatial attacks, and the sequence carried by the extracted images provides the ability to determine the type of temporal attack and localize the frames, which are tampered.

The experimental study on the method quality and efficiency is conducted. According to the results of experiments, the method is suitable for solving authentication tasks. Furthermore, the method is robust to compression and format re-encoding.

Future work is supposed to be directed towards the following issues:

1. a development of an algorithm for differentiation of attack types and automatic localization of tampered fragments;
2. an enhancement of the watermark robustness against compression by developing an improved detector for amplitude peaks;
3. a study on robustness against various types of possible geometrical attacks, like cropping and rotation.

Acknowledgements. The reported study was funded by RFBR (Russian Foundation for Basic Research): projects No. 19-29-09045, No. 19-07-00474, No. 19-07-00138, No. 20-37-70053.

References

1. Dabhade, V., Bhople, Y.J., Chandrasekaran, K., Bhattacharya, S.: Video tamper detection techniques based on DCT-SVD and multi-level SVD. In: TENCON IEEE, pp. 1–6 (2015)
2. Ghimire, S., Choi, J., Lee, B.: Using blockchain for improved video integrity verification. IEEE Trans. Multimed. **22**(1), 108–121 (2019)
3. Khelifi, F., Bouridane, A.: Perceptual video hashing for content identification and authentication. IEEE Trans. Circuits Syst. Video Technol. **29**(1), 50–67 (2019)
4. Sitara, K., Babu, M.: Digital video tampering detection: an overview of passive techniques. Digit. Invest. **18**, 8–22 (2016)
5. Aditya, B., Avaneesh, U., Adithya, K., Murthy, A., Sandeep, R., Kavyashree, B.: Invisible semi-fragile watermarking and steganography of digital videos for content authentication and data hiding. Int. J. Image Graph. **19**(3), 1–19 (2019)
6. Shiddik, L., Novamizanti, L., Ramatryana, I., Hanifan, H.: Compressive sampling for robust video watermarking based on BCH code in SWT-SVD domain. In: International Conference on Sustainable Engineering and Creative Computing (ICSECC), pp. 223–227 (2019)
7. Sharma, C., Bagga, A.: Video watermarking scheme based on DWT, SVD, Rail fence for quality loss of data. In: 4th International Conference on Computing Sciences (ICCS), pp. 84–87 (2018)
8. Alenizi, F., Kurdahi, F., Eltawil, A.M., Al-Asmari, A.K.: Hybrid pyramid-DWT-SVD dual data hiding technique for videos ownership protection. Multimed. Tools Appl. **78**(11), 14511–14547 (2018). https://doi.org/10.1007/s11042-018-6723-9

9. Barani, M.J., Ayubi, P., Valandar, M.Y., Irani, B.Y.: A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform. Multimed. Tools Appl. **79**(3), 2127–2159 (2020)
10. Guangxi, C., Ze, C., Daoshun, W., Shundong, L., Yong, H., Baoying, Z.: Combined DTCWT-SVD-based video watermarking algorithm using finite state machine. In: Eleventh International Conference on Advanced Computational Intelligence, pp. 179–183 (2019)
11. Rakhmawati, L., Wirawan, W., Suwadi, S.: A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability. EURASIP J. Image Video Process. **2019**(1), 1–22 (2019). https://doi.org/10.1186/s13640-019-0462-3
12. Solanki, N., Khandelwal, S., Gaur, S., Gautam, D.: A comparative analysis of wavelet families for invisible image embedding. In: Rathore, V.S., Worring, M., Mishra, D.K., Joshi, A., Maheshwari, S. (eds.) Emerging Trends in Expert Applications and Security. AISC, vol. 841, pp. 219–227. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-2285-3_27
13. Sujatha, C.N., Sathyanarayana, P.: DWT-based blind video watermarking using image scrambling technique. In: Satapathy, S.C., Joshi, A. (eds.) Information and Communication Technology for Intelligent Systems. SIST, vol. 106, pp. 621–628. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1742-2_62
14. Wagdarikar, A., Senapati, R.: Optimization based interesting region identification for video watermarking. J. Inf. Secur. Appl. **49**, 1–17 (2019)
15. Wagdarikar, A.M.U., Senapati, R.K., Ekkeli, S.: A secure video watermarking approach using CRT theorem in DCT domain. In: Panda, G., Satapathy, S.C., Biswal, B., Bansal, R. (eds.) Microelectronics, Electromagnetics and Telecommunications. LNEE, vol. 521, pp. 597–606. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1906-8_61
16. Tian, L., Dai, H., Li, C.: A semi-fragile video watermarking algorithm based on chromatic residual DCT. Multimed. Tools Appl. **79**(5), 1759–1779 (2020)
17. Wong, K., Chan, C., Maung, M.A.: Lightweight authentication for MP4 format container using subtitle track. IEICE Trans. Inf. Syst. **E103.D**(1), 2–10 (2020)
18. Maung, M.A.P., Tew, Y., Wong, K.: Authentication of Mp4 file By perceptual hash and data hiding. Malaysian J. Comput. Sci. **32**(4), 304–314 (2019)
19. Vega-Hernandez, P., Cedillo-Hernandez, M., Nakano, M., Cedillo-Hernandez, A., Perez-Meana, H.: Ownership identification of digital video via unseen-visible watermarking. In: 7th International Workshop on Biometrics and Forensics (IWBF), pp. 1–6 (2019)
20. Cao, Z., Wang, L.: A secure video watermarking technique based on hyperchaotic Lorentz system. Multimed. Tools Appl. **78**(18), 26089–26109 (2019). https://doi.org/10.1007/s11042-019-07809-5
21. Munir, R., Harlili: A secure fragile video watermarking algorithm for content authentication based on arnold cat map. In: 4th International Conference on Information Technology, pp. 32–37 (2019)
22. Vybornova, Y., Sergeev, V.: Method for vector map protection based on using of a watermark image as a secondary carrier. In: ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, pp. 284–293 (2019)
23. Lin, J.Y., Song, R., Wu, C.-H., Liu, T.-J., Wang, H., Kuo, C.-C.J.: MCL-V: a streaming video quality assessment database. J. Vis. Commun. Image Represent. **30**, 1–9 (2015)