Digital Watermarking Scheme of Aerial Video Data

Margarita N. Favorskaya[1], Vladimir V. Buryachenko[1], Konstantin A. Gusev[1]

[1] Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russian Federation,
{favorskaya, buryachenko, kgusev}@sibsau.ru

Abstract. The paper describes a classification of methods for digital watermarking of video sequences, as well as a classification of Internet attacks, which are divided into intentional or accidental ones. Approach for multilevel protection is based on the fragile and informative watermarks embedding. The informative watermark containing flight information, encrypted possibly, is embedded into the textural regions of a frame. The developed method for the embedding and extracting digital watermarks is invariant to the global and local geometric distortions

Keywords: digital watermarking scheme; aerial video data; copyright protection; security; capacity; robustness.

1 Introduction

Recently, digital watermarking of video materials is becoming increasingly important due to a great volume of multimedia data transmitted through the unprotected Internet networks. Digital watermarking implies the embedding of hidden digital watermarks in a view of images or textual information depending on the solved task. The goals of digital watermarking can be also different, and depending on the purpose various algorithms for embedding and extraction of the watermarks are used. The paper considers a digital watermarking of aerial video materials in order to provide a copyright protection. More complicated task is embedding the annotation results in video materials, for example the trajectory coordinates during a surveillance of object of interest, a number of moving objects, detection of forest wildfire, etc.

The structure of this paper is the following. Section 2 briefly reviews classification of the watermarking methods. Section 3 describes a multilevel protection of aerial video data. The proposed method for embedding and extraction of watermarks in aerial videos is given in Section 4. Further the experimental results are reported in Section 5. Section 6 concludes the paper.

2 Classification of Watermarking Methods

Information security of data transmission through the unprotected networks is a crucial problem in data protection. Usually, the systems of information security are divided in two main categories: encryption systems (cryptography) and information hiding (steganography and watermarking) [1]. It is considered that the steganographic methods provide additional protection for the cryptographic methods. Herewith steganography does not change a format of data or messages, as well as digital watermarking. Initially, the main function of digital watermarking was the popular copyright protection, and the main goal was creation of secure, robust, and efficient watermarks, visible or invisible, which had been embedded in media files or documents and were persistent for the unauthorized persons [2]. However, in a wide sense digital watermarking is relevant to steganography because these both approaches hide information in video data. Both approaches ought to satisfy the criteria of security, capacity, robustness, and invisibility but the priorities are set differently. For example, invisibility has a paramount meaning for steganography and at the same time digital watermarking ought first of all to provide the robustness. However, at present the complex technologies, which make it difficult to explicitly assign a method to cryptography, steganography, or digital watermarking, are developed.

Three contradictory criteria such as the hiding reliability, capacity of embedded information, and robustness to the attacks are considered during development of algorithms for embedding/extraction of the watermarks. Recently, the watermarks are considered in a wide sense, more than simple visual or textual logotypes embedding for copyright protection. Usually, the watermarks are small textual messages or a region of interest in an image. The watermarks can be fragile (destroying under all types of attacks), semi-fragile (when a part of watermark is destroyed under

attack), and robust (saving their original view generally but a degree of uniform destroy depends from the unknown parameters of attack).

The watermarks are embedded in the spatial or frequency domains of image or frame. The spatial methods are simpler in implementation but at the same time make the watermarks more visible for a human and lesser robust respect to the frequency methods. We can mention some spatial methods, i.e. method of list significant bit, difference of pixels' values, method of histogram displacement, method based on the bit planes, method based on a quantization, method based using patterns, method based on a modulation, etc. Frequency methods demonstrate greater robustness to attacks and reliable of hiding the embedded information. However, they have a volume of embedded information significantly lesser. Frequency methods for embedding hidden information are based on the transforms (discrete Fourier transform, discrete cosine transform, polar harmonic transform, discrete wavelet transform, complex wavelet transform, discrete curvelet transform, discrete shearlet transform), as well as moments (Zernike moments, pseudo Zernike moments, Chebyshev moments).

Also, the blend and non-blend watermarking schemes are possible. A blind watermarking scheme supposes that the host image or frame does not transmit through a channel, only a secrete key is transmitted. In this case, the algorithms of watermark extraction and quality estimates of its reconstruction complicate significantly.

It should be noted that the image watermarking schemes are more studied scope respect to videos watermarking schemes. If a video sequence is compressed according to one of the existing standards, then the embedding algorithms become complicated due to the limitations of compression standards. Another new area of digital watermarking schemes, having large limitations on a volume of embedded information and characterizing by large number of attacks, is a watermarking of 3D visual objects. Whenever possible, the task of 3D digital watermarking is reduced to the task of 2D digital watermarking. [3].

3 Multilevel Protection of Aerial Video Data

Multilevel protection is increasingly used in practice in response to more sophisticated Internet attacks applied to the multimedia content. It should be noted that there are a great variety of types of attacks respect to video materials. The attacks can be the intentional and accidental attacks, as it shown in table 1. The intentional attacks are directed on a distortion of a whole video sequence or single frame. The intentional attacks are divided on the common image processing and geometric attacks. At the same time, the accidental attacks are the common image processing only.

Table 1. Classification of the possible Internet attacks.

Intentional attacks				Accidental attacks
Against video sequence		Against single frame		Against video sequence
Common image processing	Geometric	Common image processing	Geometric	Common image processing
Frame dropping	Cropping	Median filtering	Cropping	Glossy copying
Frame averaging	Random bending	Blurring	Random bending	Change of frame rate
Frame swapping		Copying	Rotation	Change of resolution
MPEG compression		JPEG compression	Scaling	MPEG compression
Color distortions		Color distortions	Translation	
Contract distortions		Contract distortions	Flipping	
Noise adding		Noise adding	Composition	

Frame dropping means a removal one or several frames from the watermarked video sequence. Frame averaging distorts a motion in a scene. Frame swapping changes an ordering of frames. If a number of remote, averaged, or swapped frames is large, then a quality of video sequence becomes low. Several attacks, such as MPEG/JPEG compression, color distortion, contract distortion, and noise adding, are applied to a whole video sequence and to separate frames. Copying attack is used for frame fakes based on a textual analysis [4]. Single frame can be distorted randomly by affine transform (rotation, scaling, and shift) and also by flipping, cropping, or local random bending. Composition attacks imply a simultaneously application to frame several types of attacks. Also, the geometric attacks can be global and local attacks. Glossy copying, MPEG compression, change of frame rate or resolution are ordinary accidental attacks.

It should be noted that random manipulations with video sequences are very simple editing process. At the same time, a restoration of the distorted watermarked video sequence is a problem because the unknown parameters of distortion. At present, all existing methods of blind watermarking cannot prevent the most of distributed types of attacks. At the same time, use of non-blind watermarking requires a re-transmission of the original video sequence.

Therefore, the blind watermarking schemes are developed in the direction of multilevel protection and application of video content transforms, which are invariant to several types of attacks.

We apply three levels for frame protection. At the first level, a fragile watermark (visible, semi-visible, or invisible) WM_{FR} is embedded in the predetermined region. Usually, a fragile watermark is a logotype of company. For its embedding, it is reasonable to use discrete Hadamard transform, which does not require high computational costs [5]. Notice that the most of manipulations with content lead to partial or full destruction of this watermark.

Second level of protection means an embedding of the main watermark, for example with the flight information WM_{FI}, using one of frequency transforms, which is invariant to the most of the supposed attacks. If aerial video data are not compressed, then it is reasonable to apply discrete wavelet transform or discrete shearlet transform with a singular decomposition [6]. Also a selection of regions for embedding of hidden information has a significant meaning. The main recommendations for such selection are to choice the high textural regions, which do not attract a human attention, and the regions, where a blue component prevails because a human vision has lesser sensitivity to this wavelength range [7].

Third level of protection is the encryption of main watermark before its embedding in video content. It the main watermark is an image, then usually the reversible chaotic transforms are applied. Among them, the Arnold transform is widely used [8]. Arnold transform is a periodic reversible mapping. A number of iterations leading to appearance of the initial image is called the Arnold period. The predetermined chosen value of a number of iterations is written in a secrete key. Application of Arnold transform to the encrypted image the given times (Arnold period minus value of a secrete key) leads to the full reconstruction of initial image. Such procedure is called a scrambling procedure. If the main watermark is digital data, then we can apply the typical procedure of text data encryption (substitution, permutation), which parameters are also written in a secrete key.

4 Method for Embedding and Extraction of Watermarks

List of the main process of digital watermarking schemes is mentioned below:

– Process *GN*: the preparing of a watermark containing flight information WM_{FI} with transform to the required format and encryption if it is necessary, a fragile watermark WM_{FR}, and secrete key K. It should be noted that if any event, for example object surveillance, features of ecological disaster, or forest wildfire, is detected using additional software tools, then a watermark of event WM_{EV} is formed.

– Process *EM*: the watermarks embedding in the preliminary selected regions of a host image (frame).

– Process *EX*: the extraction of all watermarks from an image after its transmission through Internet networks using secrete key *K*.

– Process *RC*: the quality estimation of the reconstructed watermarks and reconstruction of a watermarked image if it is necessary.

Each process has its own characteristics and deserves a separate consideration. The process of embedding and extraction are reversible. However, the embedding process has a significant meaning at the sense of information hiding, as well as robustness to Internet attacks. We propose an original method of adaptive watermarking based on feature points, which is robust to the global and local geometric attacks. It is well known that feature points are robust to affine transform. If a function describing a neighborhood of a feature point on a unit circle is transformed to the function invariant to rotations (for example, using exponential moments), then the coordinates of this feature point can be embedded in this neighborhood. We recommend to apply this procedure to the restricted number of feature points, lesser 10 feature points uniformly distributed in a frame. Such method allows us to calculate the parameters of affine transform and normalize an image before extraction of the watermarks. Let us note that a fragile watermark is used at the beginning of extraction process. If a fragile watermark was not changed, then it is considered that the Internet attacks have not been applied. For fragile watermark embedding, we apply discrete Hadamard transform [5], while the main watermarks are embedded using discrete wavelet transform. Blind watermarking scheme is utilized. After compensation of global geometric distortions, the corresponding feature points are analyzed on the subject of local geometric distortions. In the case of local geometric distortions, we apply a bicubic interpolation in order to increase a quality of frame after a watermark extraction.

5 Experimental Results

For experiments, 12 video sequences obtained from a drone DJI Mavic Pro with different shooting conditions [9] were employed. The main parameters of some video sequenced from this dataset are depicted in table 2.

In each of mentioned in table 2 video sequences, we embedded the semi-visible fragile watermark and watermark in a view of logotype and then estimate a quality of reconstructed watermark after simulation of different types of attacks. For quality estimation, Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation Coefficient (NCC) metrics were used [10].

PSNR values are calculated by the following equation:

$$PSNR = 10\log_{10}\left[\frac{\mathrm{MAX}_I^2}{MSE}\right],$$

where MAX_I is the maximum possible pixel value of the frame, MSE is the mean squared error between the original and watermarked frames.

Table 2. Main parameters of test video sequences.

Caption	First frame	Resolution	Number of frames	PSNR (between the host frame and watermarked frame)
Berghouse Leopard.mp4		1280×720	1073	32.28
Bluemlisal Flyover.mp4		1280×720	957	31.23
Creux du Van Flight.mp4		1280×720	1196	30.68
Isles of Glencoe.mp4		1280×720	899	31.45
DJI_0501.mov		3840×2160	232	34.57
DJI_0574.mov		3840×2160	928	36.62
DJI_0596.mov		3840×2160	1015	34.45
DJI_0790.mov		3840×2160	1914	33.28
DJI_0862.mov		3840×2160	1450	33.45
DJI_0876.mov		3840×2160	1189	32.78

MSE is calculated by equation:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left[I(i,j) - I_w(i,j) \right]^2,$$

where m and n are the width and height of frame, respectively, I and I_W are the intensity values of the original frame and watermarked frame in coordinates (x, y), respectively.

The larger PSNR value, the lesser losses during an embedding process.

Quality of watermark reconstruction can be estimated using NCC metric:

$$NCC = \frac{\sum_{i=1}^{k} \sum_{j=1}^{l} \left[\left[w(i,j) - \mu_w \right] \times \left[\bar{w}(i,j) - \mu_{\bar{w}} \right] \right]}{\sqrt{\sum_{i=1}^{k} \sum_{j=1}^{l} \left[w(i,j) - \mu_w \right]^2} \times \sqrt{\sum_{i=1}^{k} \sum_{j=1}^{l} \left[\bar{w}(i,j) - \mu_{\bar{w}} \right]^2}},$$

where k and l are the width and height of the watermark, respectively, $w(i,j)$ and $\bar{w}(i,j)$ are the intensity values of the original and reconstructed watermarks, respectively, μ_w and $\mu_{\bar{w}}$ are the mean values of the original and reconstructed watermarks, respectively.

The NCC values change in the range [–1, +1]. A value close to 1 indicates a high degree of watermark correlation. Value close to 0 means the strong differences between the reconstructed and original watermarks that is caused by the negative impact of attacks on a video sequence.

Examples of attacks are depicted in figure 1 respect to video sequence Creux du Van Flight.mp4. The attacks simulated the typical distortions, such as the noise adding (Salt and Pepper and Gaussian noise), contract distortions, blurring, median filtering, JPEG compression, scaling, rotation, and cropping.

Table 3 shows the estimate results of extracted watermarks from aerial video sequences with different quality, viz. Creux du Van Flight.mp4, Bluemlisal Flyover.mp4, and Berghouse Leopard.mp4. The best results were obtained for video sequence Berghouse Leopard.mp4 that is explained by good quality of shooting and simple structure of a scene. Also in this video sequence, a background contains the high textural regions that are suitable for better embedding.

Table 3. Estimates of frame and watermark quality.

Types of attacks	PSNR (between the original and distorted regions of frame with a watermark), dB			NCC (between the original and distorted watermarks)		
	Video sequences					
	Creux du Van Flight	Bluemlisal Flyover	Berghouse Leopar	Creux du Van Flight	Bluemlisal Flyove	Berghouse Leopard
No attack	30.68	31.23	32.28	1.00	1.00	1.00
Rotation (15°)	29.27	29.88	31.71	0.89	0.93	0.96
Salt and Pepper (0.01)	30.33	30.89	31.33	0.97	0.99	0.98
Gaussian noise (0.01)	30.41	30.91	31.45	0.95	0.97	0.96
Intensity correction (1.2)	30.27	30.45	31.29	0.95	0.98	0.97
Blurring on motion (10, 45°)	30.21	30.37	31.10	0.96	0.91	0.95
Intensity distortion, Gaussian noise, blurring	30.13	30.22	30.89	0.91	0.85	0.92
Median filtering (3×3)	30.43	31.08	31.99	0.93	0.94	0.97
Gaussian noise (0.01) and median filtering (3×3)	30.15	30.68	31.81	0.91	0.93	0.92
Scaling (1.15)	29.86	30.76	31.11	0.83	0.86	0.89
Cropping (25%)	29.91	30.51	31.48	0.91	0.87	0.84

JPEG-compression	30.21	30.89	31.05	0.85	0.93	0.91

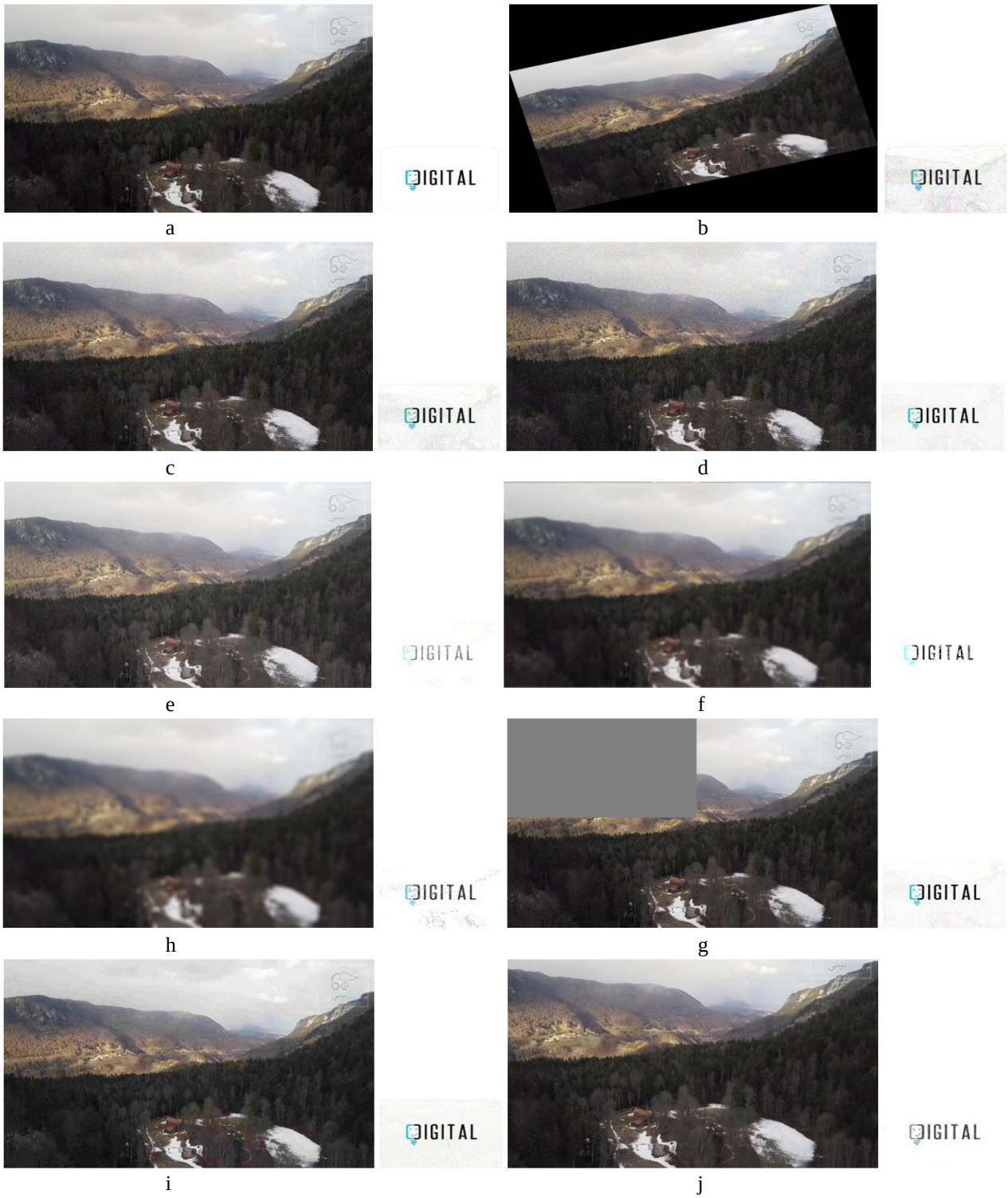

Figure 1. Examples of different types of attacks applied for video sequence Creux du Van Flight.mp4and reconstructed watermark: a original frame; b rotation, 5°; c Salt and Pepper; d Gaussian noise; e gamma-correction, increased on 20%; f median filtering; h blurring; g cropping, 25%; i JPEG-compression; j scaling

Such geometric distortions as scaling, cropping, and rotation have the greatest impact on a quality of distorted watermarks: around 19% of information is lost. At that time, the algorithm provides a high robustness to common image processing – noise, blurring, and compression. In these cases, losses are lesser 10%.

6 Conclusions

In this research, we propose a method for embedding the hidden and fragile digital watermarks in the frames of video sequences, which can be applied for digital watermarking process of aerial videos captures by the cameras of unmanned aerial vehicles and drones in order to data protection or embedding additional data, for example flight information. We developed an algorithm providing a high level of data protection using a watermark encryption and embedding a fragile watermark, which allows us to get information about Internet attacks. The conducted experiments simulating the intentional and accidental attacks show a high robustness of digital watermarks to the geometric transforms and other types of attacks, which are possible during a transmitting of video materials.

Acknowledgements. The reported study was funded by the Russian Fund for Basic Researches according to the research project № 19-07-00047.

References

[1] Cheddad A., Condell J., Curran K., Mc Kevitt P. Digital image steganography: survey and analysis of current methods // Signal Processing. 2010. Vol. 90, No. 3. P. 727-752.

[2] Shih F.Y. Digital Watermarking and steganography: Fundamentals and Techniques. 2nd edn., Boca Raton, London, New York: CRC Press, 2017.

[3] Favorskaya M.N., Savchina E.I. Digital watermarking of 3D medical visual objects // Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLII-2/W12, 2019. P. 61-67.

[4] Lu C.S., Hsu C.Y. Near-optimal watermark estimation and its countermeasure: antidisclosure watermark for multiple watermark embedding // IEEE Trans. Circuits and Systems for Video Technology. 2007. Vol. 17, No. 4. P. 454-467.

[5] Favorskaya M., Savchina E., Popov A. Adaptive visible image watermarking based on Hadamard transform // IOP Conference Series: Materials Science and Engineering, MIST Aerospace, 2018. 2018450:052003.

[6] Favorskaya, M.N., Jain, L.C. Savchina E.I. Perceptually tuned watermarking using non-subsampled shearlet transform // Computer Vision in Control Systems-3: Springer International Publishing Switzerland. 2018. ISRL, Vol. 136. P. 41–69.

[7] Favorskaya, M., Pyataeva, A., Popov, A. Texture analysis in watermarking paradigms // Procedia Computer Science. 2017. Vol. 112. P. 1460-1469.

[8] Arnol'd, V.I., Avez, A. Ergodic problems of classical mechanics. Mathematical physics monograph series. New York, Benjamin, 1968. 286 P.

[9] Drone Videos DJI Mavic Pro Footage in Switzerland https://www.kaggle.com/kmader/drone-videos

[10] Sachin, G., Vinay, K. A RDWT and Block-SVD based dual watermarking scheme for digital images // Int. J. Advanced Computer Science and Applications (IJACSA). 2017. Vol. 8, No. 4. P. 211-219.