The Performace Evaluation of GMSAT Video Watermarking against Geometric Attacks

Zoran Veličković[1], Zoran Milivojević[1] and Marko Veličković[1]

Abstract – **In this work, the performance of the algorithm GMSAT protection of original video content in relation to the geometric malicious attacks are determined. The goal of geometric attacks on video is to disable the watermark extraction, thus endangering the copyrights. The paper analyses geometrical attacks realized by the addition of noise, filtering and cropping the parts of the video frames. The GMSAT algorithm showed good resistance to discussed geometric attacks so that it can be recommended for the protection of original video content before exposure on the Internet.**

Keywords – **Generalized Multistage Arnold Transformation, Watermarking, Geometric attacks.**

I. INTRODUCTION

This paper discusses the algorithms for protecting original multimedia content from illegal copying and distribution. In a network environment of modern broadband Internet, protection of multimedia content, especially video, is becoming an indispensable activity of the author prior to publication on the Internet. In 2016, 64% of all Internet transmitted packets related to some form of video traffic [1]. Contemporary online multimedia applications, a special VoIP (Voice over Internet Protocol), VOD (Video on Demand) and video conferencing have contributed to the enormous increase in packet traffic. Adoption of the new standard high-resolution video such as HD, 4K UHD and will only increase the share of video packets in global IP traffic. Required network bandwidth for transmission of 4K video is twice that of HD resolution, that is, nine times higher than the SD resolution. In [1] is presented astonishing assumption that by the end of 2019 the share of the total video packets in IP traffic to increase to 80%.

These data clearly indicate that the exchange of digital multimedia content, especially video, has already become the dominant form of IP traffic. Trends in modern multimedia communication technologies for the researchers set new, previously unknown tasks and challenges [2], [3]. The ubiquitous availability of digital multimedia content, as well as their properties when copying there is no drop in quality, are favored piracy occurs. Copyright protection of digital multimedia content in the aforementioned network conditions is a very complex task [4].

[1]Zoran Veličković is with College of Applied Technical Sciences, Nis, Serbia, A. Medvedeva 20, 18000 Niš, Serbia, E-mail: zoran.velickovic@vtsnis.edu.rs

[1]Zoran Milivojević is with College of Applied Technical Sciences, Nis, Serbia, A. Medvedeva 20, 18000 Niš, Serbia, E-mail: zoran.milivojevic@vtsnis.edu.rs

[1]Marko Veličković is with College of Applied Technical Sciences, Nis, Serbia, A. Medvedeva 20, 18000 Niš, Serbia, E-mail: marko.velickovic93rsni@yahoo.com

In order to prevent illegal copying and distribution of digital multimedia content on the Internet can be applied standard cryptographic techniques. However, although by standard cryptographic techniques based on PKI (Public Key Infrastructure) are very reliable, they are not adequate for the protection of multimedia content. The main drawback of these techniques is reflected in the necessary decryption before playing multimedia content, which content exposes to security risks. For practical application are more convenient methods which are based on inserting a watermark in the multimedia content [5]-[9]. Methods of protection of multimedia content based on the watermark insertion means the permanent insertion of the multimedia content so that it does not remove during playback. This concept of protection of multimedia content indirectly protects watermark itself from malicious and destructive attacks. In this way, further increases the level of security of protected multimedia content.

The knowledge of the watermark content in some cases can threaten the security of the protected video. Therefore, in this paper it is proposed to use a GMSAT (Generalized MultiStage Arnold Transformation) for encrypting - scrambling of the contents of the watermark [6], [7]. To obtain the original watermark from scrambled, it is developed inverse algorithm IGMSAT. Just knowing all the parameters of IGMSAT it is possible to transform scrambled watermark in the original. Since the algorithm belongs to a class GMSAT invertible chaotic maps it is necessary to know the initial conditions of transformation.

In this article, the insertion of the watermark in scrambled video content reliable algorithm based on a combination of a DWT (Discrete Wavelet Transform), and SVD (Singular Value Decomposition) is applied. Scrambled watermark is embedded into each frame of uncoded video sequences. It should be noted that after the insertion of scrambled watermark, video are coded by H.264 / AVC encoder. Given that, the H.264 / AVC encoder belongs to a class encoder with losses in coding inevitably leads to degradation of video content, and thus the inserted watermark. The influence of the applied encoder on video content and quality of the extracted watermarks are analyzed in previous papers of authors [5]-[8].Also, the prior papers of authors tested the resistance of the used techniques to false tripping of the watermark and lack of knowledge of a set of transformation parameters [6].

This paper especially analyzed malicious attacks which can be classified into geometrical attacks. Because the geometric attacks impact destructively on protected video, the survival of the inserted watermark after these attacks are analyzed. One part of the analysis consists of adding the Gaussian and "salt & pepper" noise, while the second part of the analysis relates to a median filtering, and the tear-off parts of the protected decoded video content.To improve the extracted watermark, advanced corrections algorithm based on a set of

extracted variable quality watermarks is used. In this article it is experimentally confirmed the robustness of the proposed algorithm, which includes insertion, extraction and improvement of quality of the watermark to its removal attempts.

The second section presents a mathematical basis of GMSAT, while the third section provides reliable modified algorithms for installation and extraction of the watermark based on DWT and SVD. Fourth section evaluate the proposed algorithm and shows the results of the performed experiments. Based on the analysis results, the robustness of the algorithm on some geometric attacks is verified. In the fifth chapter an appropriate conclusions on the basis of the tests are conducted.

II. Generalized Multistage Arnold Transformation GMSAT

In the prior papers authors are suggested MSAT (MultiStage Arnold Transformation) [7] for scrambling the content of the watermark. The basic idea of this transformation is based on the sequential application of multiple Arnold transformation - stage of the watermark. The transformation parameters of i-th stagea_i, b_i, and the number of sequential iteration k_i represent the keys for the encryption, while the period of Arnold transformation stage T_i further demands for the application of inverse MSAT-a. This paper applies GMSAT (Generalized Multistage Arnold Transformation), which allows variations dimensions square watermark N_i in stages [6]. Each stage of a generalized 2D multistage Arnold transformation (i) can be described by the expressions (1) and (2):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & b_i \\ a_i & a_i b_i + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \right) mod N_i \quad (1)$$

$$N_i \leq N, i \in (1, 2, \dots I)$$

$$(x, y) \in (0,1, \dots, N_i - 1) \times (0,1, \dots, N_i - 1) \subset Z^2 \quad (2)$$

where x_n, y_n i x_{n+1}, y_{n+1}represent the locations of image pixels, and a_i, b_i and N_i are parameters of multistage Arnold transformation. Set parameters Key_I which determine a generalized multistage Arnold transformation can be represented by the expression (3):

$$Key_I = f\left(E_i\left(a_i, b_i, k_i, N_i, T_i\right)\right), i = 1,2, \dots I \quad (3)$$

where E_i represents the i-th stage of the I-th GMSAT stages. When scrambling locations pixels watermark by GMSAT, on the input of the first stage E_1 brings the original watermark, and the exit from I-th E_I stage gets transformed watermark. When using IGMSAT (Inverse GMSAT) procedure shall be repeated with the same parameters but in reverse order. Scrambled watermark is fed to an inverse algorithm as well as the stages I-th IE_I, while the original watermark obtained at the output of the first stage of the inverse algorithm of IE_1. Similarly to GMSAT, the output of the previous stage IGMSAT are fed to the following stages of IGMSAT.The capacity of the inserted watermark is equal to 25% of the video frame size.

III. Reliable Algorithm for Watermark Insertion and Extraction

In this work, the insertion and extraction of the watermark in the video frame in the SVD domain performs by reliable algorithm. Reliable SVD algorithm solves the problem of false positives watermark which is inherent in standard SVD algorithm. Details of the algorithm for insertion and extraction of encrypted watermark in the DWT-SVD domain [6], [9] are represented by a series of the following steps I and E.

A. Algorithm for Watermark Insertion

Step I_1: Decomposition of the frame $\boldsymbol{F}$ by using the second-level DWT transformation:

$$\{\boldsymbol{F}^k, \boldsymbol{F}^l\} = DWT_{2_{Haar}}(\boldsymbol{F}) \quad (4)$$

$$k \epsilon \{LL_2, HL_2, LH_2, HH_2\}$$

$$l \epsilon \{HL_1, LH_1, HH_1\}$$

Step I_2: SVD decomposition sub-band $\boldsymbol{F}^k$, k=LL_2:

$$\boldsymbol{F}^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_F^k \cdot (\boldsymbol{V}_F^k)^T . \quad (5)$$

Step I_3: Encrypting the original watermark $\boldsymbol{W'}$ (lower resolution) using a generalized multi-step transformation of Arnold's and the preparation of a watermark $\boldsymbol{W}$ which is inserted into each frame.

$$\boldsymbol{W} = \underset{E_i(a_i, b_i, k_i, N_i, T_i)}{Gen\_Arnold}(\boldsymbol{W'})$$

$$i = 1,2, \dots I . \quad (6)$$

Step I_4: SVD decomposition encrypted watermark $\boldsymbol{W}$ and calculating the principal components$\boldsymbol{A}_{\text{wa}}$[8].

$$\boldsymbol{W} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w \cdot \boldsymbol{V}_w^T = \boldsymbol{A}_{wa} \cdot \boldsymbol{V}_w^T ; \boldsymbol{A}_{wa} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w . \quad (7)$$

Step I_5: Installation of principal components $\boldsymbol{A}_{\text{wa}}$ in a diagonal matrix sub bands$\boldsymbol{S}_F^k$ by a factor of inserting α:

$$\boldsymbol{S}_{F\_1}^k = \boldsymbol{S}_F^k + \alpha \cdot \boldsymbol{A}_{wa} . \quad (8)$$

Step I_6:Creating a modified sub-band with embedded watermark:

$$\boldsymbol{F}_w^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_{1\_F}^k \cdot (\boldsymbol{V}_F^k)^T . \quad (9)$$

Step I_7:Replacing the original sub-band of second frame level by a modified and application of the inverse discrete wavelet transform $IDWT_2$ for obtaining watermarked frame.

$$\boldsymbol{F}_w = IDWT_{2_{Haar}}(\boldsymbol{F}_w^k, \boldsymbol{F}^l) . \quad (10)$$

B. Algorithm for Watermark Extraction

The process of extracting a watermark $\boldsymbol{W}^*$ from a protected video can be done by following the steps E:

Step E_1: Decomposition of the original frame $\boldsymbol{F}$ by using the second-level DWT transformation:

$$\{\boldsymbol{F}^k, \boldsymbol{F}^l\} = DWT_{2_{haar}}(\boldsymbol{F}) \quad (11)$$

$$k \epsilon \{LL_2, HL_2, LH_2, HH_2\}$$

$$l \epsilon \{HL_1, LH_1, HH_1\}$$

Step E_2: SVD decomposition sub-band $\boldsymbol{F}^k, k = LL_2$

$$\boldsymbol{F}^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_F^k \cdot (\boldsymbol{V}_F^k)^T \quad (12)$$

StepE_3: Decomposition of the potentially attacked frame by using the second-level of DWT transformation:

$$\{\boldsymbol{F}_w^{*k}, \boldsymbol{F}_w^{*l}\} = DWT_{2_{haar}}(\boldsymbol{F}_w^*) \quad (13)$$

Step E_4: SVD decomposition sub-band $\boldsymbol{F}_w^{*k}$:

$$\boldsymbol{F}_w^{*k} = \boldsymbol{U}_{Fw}^{*k} \cdot \boldsymbol{S}_{Fw}^{*k} \cdot (\boldsymbol{V}_{Fw}^{*k})^T \quad (14)$$

StepE_5: Creating a difference of original ($\boldsymbol{F}^k$) and the protected frame ($\boldsymbol{F}_w^{*k}$):

$$\boldsymbol{F}_1^k = \boldsymbol{F}_w^{*k} - \boldsymbol{F}^k \quad (15)$$

Step E_6: Determination of principal components:

$$\boldsymbol{A}_{wa}^{*k} = \frac{\left(\boldsymbol{U}_F^k\right)^{-1} \cdot \boldsymbol{F}_1^k \cdot \left(\boldsymbol{V}_F^T\right)^{-1} \cdot \left(\boldsymbol{V}_F^k\right)^T}{\alpha} \quad (16)$$

Step E_7: Calculation of the inserted encrypted watermark $\boldsymbol{W'^*}$ is done as follows:

$$\boldsymbol{W'^{*k}} = \boldsymbol{A}_{wa}^{*k} . \boldsymbol{V}_w^T \quad (17)$$

Step E_8: Decrypting the original watermark $\boldsymbol{W^{*k}}$by the inverse transformation of the generalized multistage Arnold transformation and obtaining the original of the watermark $\boldsymbol{W^{*k}}$:

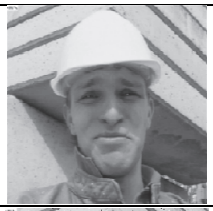
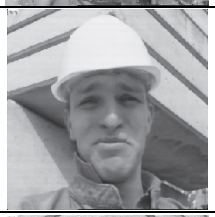
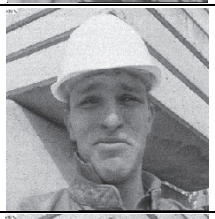
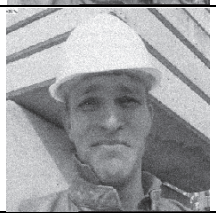
$$\boldsymbol{W}^{*k} = \underset{E_i(a_i, b_i, k_i, N_i, T_i)}{Inv\_Gen\_Arnold}(\boldsymbol{W'^{*k}})$$
$$i = 1,2, \ldots I \, . \quad (18)$$

IV. Experiments and Results

In the experimental part of this work, the central part of the famous painting "Lena.bmp" at a resolution of 72 × 72 pixels is used as a watermark. In order to increase the level of protection, the content of the watermark is scrambled by G4SAT with parameters: a [2 1 4 3], b [2 1 2 1], N [72 60 50 72] to [9 5 7 7] and T [12 60 18 18]. Watermark obtained after fourth stage represents the scrambled watermark inserted in the first 50 frames of a video "Foreman." The output from the previous step in G4SAT-a is input to the next stage, which defines the sensitive initial conditions of the transformation. To restore scrambled watermark in the original, it is necessary to know all the parameters of all stages and the initial conditions of each stage. Insertions scrambled watermark in all frames of the video is carried out as described by reliable SVD algorithm with a constant insertion factor α = 0.05. In this paper, the scrambled watermark insertion in DWT-LL2 sub-band of each frame is conducted. After protection of the video it is coded by reference software JM of ITU in version 18.4. – FRExt. Quality of coding is defined by a set FRExt parameters. A key influence on the selection of quality encoding has the following parameters:*IntraPeriod*=12, *NumberReferenceFrames*=5 *NumberBFrames*=1.

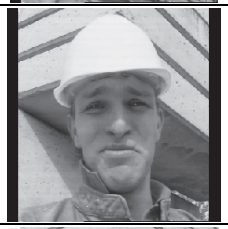
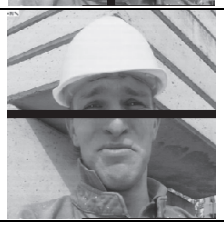
The performance of the proposed algorithm are tested on the first 50 frames of the famous video "Foreman". The first 50 protected and encoded frames of this video are decoded and then they are exposed to some of the geometric attacks. In

TABLE I
VARIOUS NOISE ATTACKS ON WATERMARKED VIDEO "FOREMAN"

Attack	Watermarked video Foreman	Watermark	MSSIM	NC
No			0.8956	0.9852
salt & peppernoise density 0.01			0.4104	0.7186
Median filtering			0.4104	0.7155
Gaussian noise variance 0.001			0.5493	0.8525
Gaussiannoise variance 0.002			0.4300	0.7464

Tables I and II are shown the geometrical attacks that were applied to the frames in this paper. The presented algorithm for the extraction from protected and attacked frames can extract a set of variable quality watermarks. In order to improve the extracted watermark, an advanced algorithm for correcting the quality is applied [8]. The quality of extracted watermarks was evaluated by SSIM (Structural Similarity) and NC (Normalized Correlation) index. The first column in the Tables I and II represent the types of the applied attack, while in the second columns of the table the attacked frames from which to be extracted watermarks are shown. In the third column of the table shown by the appearance of the extracted watermarks for individual attacks, while the fourth and the fifth column shows the calculated MSSIM and NC index of extracted and corrected watermarks. In the first row of the table I are shown the results obtained when the frame is not applied to any attack. The results shown in the first row of Table I should be used as a reference against which to assess the performance of the proposed algorithm.No significant CPU load compared to similar algorithms.

TABLE II
VARIOUS CROPPING ATTACKS ON WATERMARKED VIDEO "FOREMAN"

Attack	Watermarked video Foreman	Watermark	MSSIM	NC
Missing 15 pixels from one side			0.3396	0.6227
Missing 15 pixels from each sides			0.2478	0.4782
Missing block 15x15 pixels			0.3528	0.6302
Missing 10 pixels, vertical			0.4738	0.7665
Missing 10 pixels, horizontal			0.0892	0.1158

At the beginning it should be noted that due to the rounding of the applied mathematical transformations and effects coding encoder with losses, it is not possible to extract the watermark with maximum coefficients SSIM and NC. Table I refers to attacks related to the additive noise and filtering, while Table II applies to attacks to remove certain parts of the frame.

The analysis of the results shown in Table I may be seen that the different attacks have different impacts on the quality of the extracted watermark. The applied "salt & pepper" noise ratio (density = 0.01) and the median filter are lowered quality of the extracted watermark to 31.56%, while the effect of the Gaussian noise will lower the quality of the extracted watermarks to 38.67% (variance = 0.001), respectively, 51.99% (variance = 0.002). In Table II are presented the results of geometric attacks based on removing parts of the frames. The proposed algorithm is significantly more resistant to lack of pixels vertically in relation to the lack of pixels horizontally. Cropping decoded frame on the one side vertically lowers the quality of the extracted video for 62.08% and 72.33% from cropping two sides. Cropping in the center of the frame causes a lowering the quality of 60.6% and 47.1% for the lack of a central vertical. The lack of a central horizontal significantly lowers the quality of the extracted watermark. The proposed algorithm is unresisting to this type of attack because the extracted watermark can not be recognized. In all other considered attacks watermark is detectable and can be successfully extracted from attacked video.

V. CONCLUSION

In this work, the performance of the algorithm to protect video watermark in an attempt geometric malicious attacks are determined. A watermark is inserted in unencoded domain, so it is independent of the compression standards. The content of the watermark is scrambled before insertion in all video frames using GMSAT, while the insertion by reliable algorithms based on DWT and SVD transformations is performed. After protection, video is coded, and in the experimental part of the work has demonstrated resilience of the proposed algorithm on most geometric attacks. The only drawback of this algorithm is expressed in the geometric attack when horizontal area of 10×288 pixels is destroyed. This deficiency can be attributed to characteristics SVD transformation. In all other cases the geometric attacks, watermarks were extracted with acceptable quality. The quality of the extracted watermarks measured by SSIM index ranged from 0.2478 to 0.5493, while the NC ranged from 0.4782 to 0.8525. The obtained results are in accordance with a similar algorithms. The presented algorithm showed good resistance in geometric attacks based on adding noise, filtering and cropping, so it can be successfully applied in the protection of original video content on the Internet.

REFERENCES

[1] Cisco White Paper, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020", Feb. 2016.

[2] M. Jevtović, and Z. Veličković, *Kvalitet usluga digitalnih mreža*, Akademska misao, Beograd, 2014.

[3] L. Cai, X. Shen, J.W. Mark, *Multimedia Services in Wireless Internet: Modeling and Analysis*, John Wiley & Sons, 2009.

[4] R. Ahuja, and S. S. Bedi, "All Aspects of Digital Video Watermarking Under an Umbrella", *I.J. Image, Graphics and Signal Processing*, vol. 12, pp. 54-73, 2015.

[5] Z. Veličković, Z. Milivojević, and M. Veličković "The Insertion of the Encrypted Low-Resolution Watermark in the Uncompressed Video", *ICEST 2016*, pp. 191-194, Ohrid, 2016.

[6] Z. Veličković, and M. Veličković, "Bezbednost videa žaštićenog vodenim žigom skremblovanim GMSAT algoritmom", *INFOTEH*, Jahorina 2017.

[7] Z. Veličković, M. Veličković, Z. Milivojević, "Improved Gray-scale Watermark Encryption Based on Chaotic Maps", *UNITECH 2016*, pp. II-145-150, Gabrovo, 2016.

[8] Z. Veličković, Z. Milivojević, M. Veličković, and M. Jevtović, "The Impact of Prediction Structures H.264 Encoder on the Quality of the Extracted Watermark from the Chaos Domain", *ETF Jour. of Electrical Engineering*, vol. 22 , pp. 111-121, Podgorica, 2016.

[9] R.M. Ibrahim, N. Kader, and M. Zorkany, "Video Multiple Watermarking Technique Based on Image Interlacing Using DWT", *The Scientific World Journal*, Hindawi, vol. 2014.