Video Watermarking using Bit-plane Decomposition in Chaos domain

Zoran Veličković, Zoran Milivojević
College of Applied Technical Sciences
Niš, Serbia
zoran.velickovic@vtsnis.edu.rs

Marko Veličković
College of Applied Technical Sciences
Niš, Serbia
marko.velickovic93nirs@yahoo.com

Abstract— **In this paper, a watermark for the protection of video content was used. Prior to inserting into the video, the watermark was decomposed into two 4-bit-planes, which are scrambled by GMSAT algorithm. Insertion was performed in the DWT-SVD domain with a reliable algorithm. The quality of the protected and then encoded video is satisfactory and it is on the level of previously published results. At the same time, the quality of the extracted watermark is good and it can be used in the processes of proving ownership. In relation to known algorithms, the advantage of the proposed algorithm is its safety, which it provides thanks to bit-plane decomposition and scrambling the watermark.**

Key words – Bit-plane decomposition; DWT; GMSAT; SVD; Watermark.

I. INTRODUCTION

A growing number of modern companies are based their business models on the intensive use of ICT (*Information and Communication Technologies*) [1]. Especially attractive are business models that enable access to online data for their mobile users. The business concept based on the Internet, especially on mobile platforms, dominated in 2017. At the end of 2016, for the first time, a greater number of Internet access through mobile platforms was achieved in relation to all other ways of access. In 2017, there was a significant increase in the growth of Web access through the IoT (*Internet of Things*) module in M2M (*Machine-to-Machine*) communications. Security, automation of buildings and smart metering of utility services are very important trends in the M2M communication segment [2].

Satisfying QoS (*Quality of Services*) in a mobile environment is significantly more difficult than in wired communications. Therefore, the design of modern Web applications must be optimized for use in a mobile environment. A number of new Web technologies have been developed that put mobile technologies in first plane [3]. Even Web applications are developing first for mobile platforms and then thay are adapted for desktop computers. In order to provide a satisfactory user experience QoE (*Quality of Experience*) in the use of the mobile Internet, a common optimization of all network protocols on the ISO/OSI stack must be performed [4].

Modern mobile applications provide access to different content, but multimedia contents are the most interesting for users. When multimedia content is being exchanged, it requires the occupation most of available network resources. This fact can lead to the emergence of some network-dependent applications becoming "hungry" data, and it is difficult to provide the appropriate QoS in these conditions.

Modern Web technologies have provided the opportunity to access high quality real-time content, which has led to the occurrence of new security and control systems based on video streams. Thus, systems for remote monitoring of patients after surgical interventions have been developed. A large number of companies have provided the possibility of direct security video surveillance of remote facilities and installations. In addition to the video surveillance system, there are especially popular systems for sharing digital video content, such as *YouTube* Web portal, that is, film and TV content such as *Netflix*.

The global availability of digital multimedia content, as well as tools for their processing and storage, has led to the occurrence of illegal online activities. Illegal activities are primarily associated with unauthorized copying and illegal distribution of music, film and video on the Internet. This paper presents the protection of copying and illegal distribution of videos in modern network conditions. It can be said that the protection against copying and illegal distribution of multimedia content is a standard activity before each public release [5]. The use of standard cryptographic techniques over multimedia content does not provide the necessary copy protection level.

The use of standard cryptographic techniques over multimedia content does not provide the required copy protection level. Standard cryptographic techniques effectively protect multimedia content at the time of their transport through communication channels. On the receiving side, this technique implies the process of decrypting and knowledge of the used cryptographic keys. The basic lack of standard cryptographic techniques lies in the fact that once decrypted multimedia content can be further illegally copied and distributed.

On the other hand, the decryption process are executed during the entire time of multimedia playback and occupate processor and memory resources on the receiving terminal. With mobile devices, activating additional processor resources causes increase power consumption, which again requires a higher battery capacity of the mobile device. With the development of mobile technologies, the consumption problems are being addressed in an increasingly efficient way. Low-power processors with multiple cores are developing, the capacity of

batteries is growing and their charging becomes more efficient. In addition, satisfying QoS in a mobile environment is difficult by the potential for frequent packet loss. In multimedia applications, a certain packet loss level can be tolerated, but the delay is almost impossible to tolerate [4]. These are the reasons that make it difficult to implement the necessary QoS video applications in a mobile environment. The mentioned problems in the realization of video content protection on the Internet, have led to the new protection technologies. These technologies are not based on encryption of video content but on the insertion of a watermark into the video content itself. An arbitrary image (the company's most common logo) is invisibly inserted into video content. This concept implies that the insertion of a watermark should not cause visible degradation of the video, because it permanently stays in it. If a watermark can be extracted from the protected video, then the ownership of the video content is shown [6].

The extracted watermark should have satisfactory quality in order to use for proving ownership. It is known that a stronger inserted watermark provides extraction of a better quality brand, but at the same time causes more degradation of the video (and vice versa). Algorithms for inserting and extracting the watermark should optimally determine the insertion power to satisfy these two opposite requirements. Numerous methods that optimally determine the value of the insertion factor taking into account the types of malicious attacks on multimedia content have been developed [7].

The protection of multimedia content is the current topic of many researchers. A number of algorithms with specific characteristics for different applications have been published. In order to have practical algorithms, for each watermark insertion algorithm, an inverse algorithm for its extraction should be realized.

In order to increase the safety of the watermark and its resistance to malicious attacks, in this paper the decomposition of the watermark to the so-called "bit-plane" was applied. The decomposition of the watermark at multiple "bit-planes" allows its dissemination in multiple video frames. Unlike previously published works when the same picture is inserted in each frame, this is not the case here. Namely, only one bit-plane is inserted into a series of successive frames.

In general, the bit-planes are very different one from another. The direct consequence of the watermark decomposition at multiple bit-planes is the reduction of the required frame insertion capacity. This also reduces the visible artifacts in the video.

In [8], bit manipulation was used to hide information embedded in images. In the insertion procedure, additive bit-plane manipulation was used to increase the robustness of the algorithm and retain good visual quality. To insert a watermark, lossless integer transform was used. Better regions are selected in the cover picture. In [9], a black-and-white watermark decomposition in 8 bit-level was performed in a similar manner as in this paper. Each bit-plane is inserted into a special frame of video sequences, while in this paper two Hi and Lo bit-planes are inserted. Insertion was performed in the DCT domain as opposed to this work where the insertion is done in the DWT-SVD domain. The scrambling of the watermark has not been performed, while in this paper, the GMSAT algorithm is used for scrambling decomposition of the bit-planes. In [10] the proposed algorithm decomposes input images into *bit-planes*, randomly swaps bit-blocks among different bit-planes, and conducts XOR operation between scrambled images and secret matrix controlled by a chaotic map. The Henon map is used for encryption, while in this paper the GMSAT algorithm for watermark encryption is used.

Good features of chaotic maps for scrubbing watermark content are also applied in this paper. Scrambling in this case is performed over every bit-plane using a GMSAT chaotic map [11]. In fact, eight different - scrambled images, consisting of a watermark, are inserted into consecutive frames. On the receiving side, scrambled bit-planes that represent only one component of the watermark are extracted from decoded video frames. In order to get the original bit-planes to which the original watermark can be compiled, it is also necessary to know the parameters of the inverse GMSAT algorithm [12].

The second chapter gives an overview of the watermark insertion algorithms. Basic advantages and disadvantages of individual algorithms are presented. The third chapter describes the watermark pre-treatment algorithm prior to incorporation into frame video. The decomposition of the watermark to the bit level is described and it is briefly shown GMSAT algorithm for scrambling. The fourth chapter shows the insertion of decomposed and scrambled watermarks into video frame in the DWT-SVD-GMSAT domain. In the fifth chapter, the obtained results of the performed experiments are presented, and in the sixth chapter conclusions based on the obtained results are presented.

II. OVERVIEW OF INSERTING ALGORITHMS

In the literature, we can find more classification of techniques for inserting and extracting watermarks on various bases [13]. One of the basic classification is on techniques that produce a *visible* or *invisible* watermark. In the past, a visible watermark was used as an easy way to designate ownership of multimedia content. The problem with this technique is that a visible watermark can be removed from the multimedia content using simple video processing techniques. On the other hand, an invisible watermark is now more used to protect multimedia content from copying and illegal distribution. An invisible watermark can be used to protect multimedia content in many ways. In one scenario, the watermark degradation is required when attempting to extract it from multimedia content (*fragile*), and in the second one, the survival of the watermark in multimedia content when encoding multimedia content (*semi fragile*) is required. The watermark's resistance to degradation of multimedia content and attempts to remove it are very important requirements (*robust*).

If the process of detection and extraction of a watermark does not require possession of original multimedia content or watermark, then these techniques are called *blind* techniques. If in the process of watermark extraction, the original multimedia content or watermark is required, then these techniques are called *non-blind* techniques.

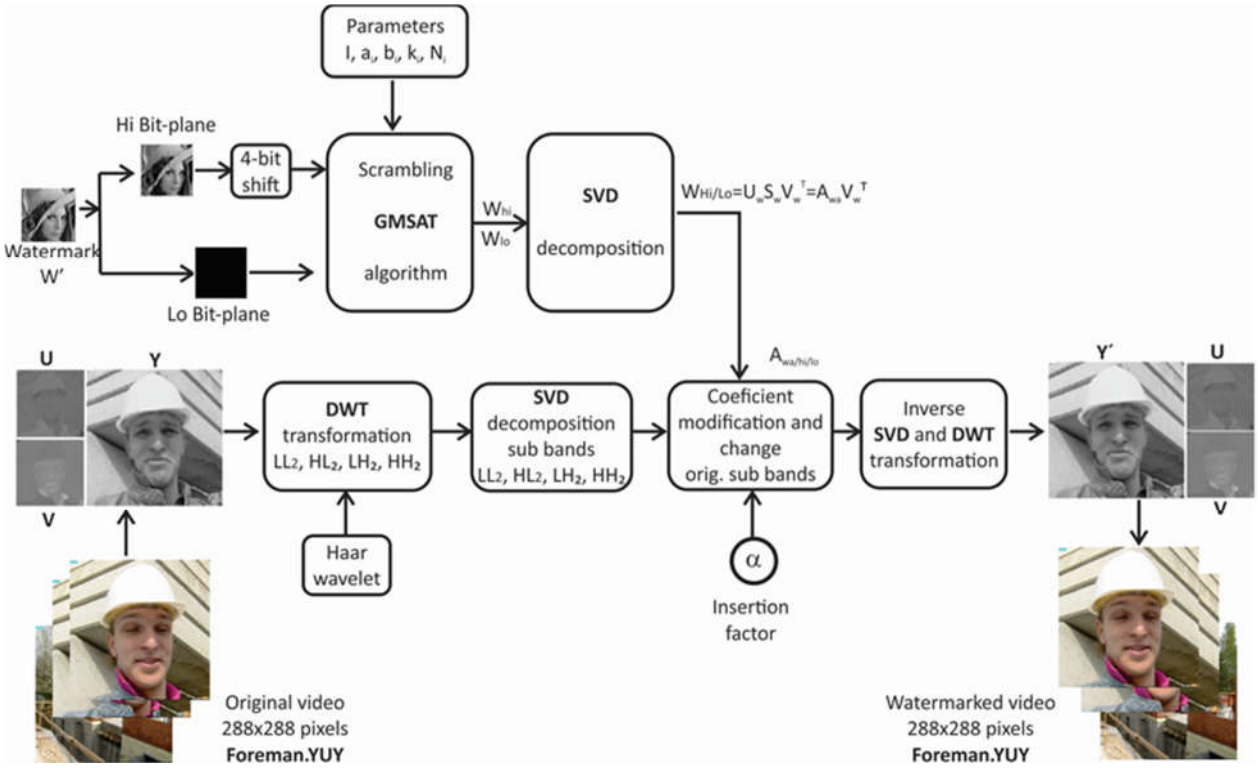


Fig. 1. Algorithm for decomposition, scrambling and inserting a watermark into video content.

If only some parameters of the original in the extraction process are required, then these techniques are called *semi-blind* techniques.

The basic characteristic of all multimedia content is the large amount of data that needs to be stored in some way. It is known that multimedia content has a high redundancy of data, so that by researching similarities, the amount of data for their presentation can be significantly reduced. If compression algorithms ignore some details in multimedia content, then it is about coding with losses. These encoding algorithms adversely affect on watermarks extraction and often it cannot be extracted from decoded multimedia content with satisfactory quality. Video content is specific in that it has a large redundancy of data in the time and space domain, so that potentially high compression rates can be achieved. A large number of encode (compression) techniques have been developed for storage and transfer of multimedia content. Thus, a large number of techniques have been developed for inserting a watermark in both unencoded and in the compressed (encoded) domain.

It is clear that inserting a watermark in the compression domain depends on the encoder specificity and it can not be applied to all other encoders. This characteristic of compression domain watermarking can be considered like a major disadvantage, since special algorithms for each codec used must be developed. Thus, for example, when inserting a watermark in the H.264/AVC codec, the encoder can take into account the intra, that is, the interframe prediction that other codecs do not have to have. In order to efficiently apply watermarking algorithms to an unencrypted domain, the survival of the watermark must be ensured after the application of complex compression algorithms. Depending on the transformation domain where the insertion or extraction of the watermark is performed, the techniques are divided into *spatial* (direct) and *transformational* (frequency). With spatial methods, the watermark is inserted directly into the pixel values of the cover image, or the frame in the video.

Unlike of spatial – direct methods, the watermark is inserted into the transformation coefficients domain in case of frequency methods. The most commonly used frequency methods in video processing are: *Contourlet*, YCbCr, FFT (*Fast Fourier Transformation*), SVD *(Singular Value Decomposition*) , and DWT (*Discrete Wavelet Transform*) so that the literature can provide examples of inserting watermarks in the corresponding transformation coefficients. In order to take advantage of the good properties of certain transformation techniques, the methods are combined to form the so-called *hybrid* technique. In general, it can be said that transformation methods are more robust to malicious attempts to remove because the watermark is scattered across the entire cover image.

III. WATERMARK PRE-PROCESSING

A watermark inserted into multimedia content can be in *color*, *monochrome* (black and white - grayscale) with 256 levels of gray or *binary* images in which each pixel is represented with only two values. In RGB color space, three bytes are used (one for each of the basic colors) to represent the color of each individual pixel. For each pixel in black and white images, one byte is reserved, while only one bit is reserved for binary images. The insertion of a color image should provide a large insertion

capacity which often exceeds the possibilities of the method and causes the cover image to degrade. This is the reason why binary or black and white images are usually inserted. This choice has no major drawbacks in the process of recognizing an extracted watermark. Most of published methods refer to the insertion of black and white images into multimedia content. One way to increase the resistance of inserting a black and white image in a mobile environment is to share the image in multiple bit-planes. The basic idea is to make protected video more resistant to packet loss in a mobile environment.

A. Bit-plane watermark decomposition

The standard mode of memorizing unencoded monochrome images (even watermarks) is in the matrix form of m × n dimension. The elements of this matrix represent the illumination of each individual pixel of the watermark. The matrix elements in this case are non-negative integers d that can be represented in the position binary system with n bits:

$$d = \sum_{i=1}^{n} b_i \, 2^{i-1}. \quad (1)$$

For a monochrome image, the pixel values are in the range $0 \leq d \leq 255$ so that each pixel value can be represented by an 8-bit binary number ($i = 8$). The expression (1) allows the monochrome image decomposition into eight bit-planes. One bit-plane is formed from the corresponding weight bits of all the pixels of the watermark [7]. Thus, *i*-th bit-plane is formed from the *i*-bits of all pixels of the watermark. Visual information at higher bit-planes is more significant than those on lower bit-planes. This fact actually favors the insertion of higher bit-levels because they significantly influence the recognition of the watermark. At the same time, the required capacity of the insertion method can be reduced. On the other hand, the decomposition of the watermark into multiple bit-planes allows the insertion of individual bit-plane of watermark in several video frames. Watermark dissemination in eight video frames will favorably affect the identification of a watermark in the event that some of the frames are lost or degraded. This increases the robustness of the algorithm to unwanted attacks. Later, on the receiving side, the complete watermark can be formed of all extracted watermark's bit-planes according to the expression (1).

It is also possible to combine multiple bit-planes into one common bit-plane, which can further reduce the insertion capacity. In this paper, this possibility has just been used. A group of 4 MSB bits in a single 4-bit-plane was formed which called Hi-bit plane. Also, another 4-bit-plane was formed from the remaining bits of 8-bit decomposition.This 4-bit plane is called Lo-bit plane.

In terms of how they are obtained, the numerical values of the pixels in the Hi-bit plane are considerably greater than those in the Lo-bit plane. In order to reduce the impact of higher pixel values on the degradation of protected video, all the values in the Hi-bit plane for the four positions to the right have been shifted.

B. Watermark scrambling

Before inserting a watermark (no matter what form it is inserted) it can be made to an observer unrecognizable. The reason for this can be found in the security aspect. Chaotic 2D maps are the most commonly used transformation that can make the watermark seem pseudo-random [5], [6], [10], [11]. The basic idea of chaotic 2D maps is to relocate the pixels of the original image for the purpose of spatial decoration of adjacent pixels, making the original picture unrecognizable. The transformed image seems seemingly random even though it was obtained by a deterministic algorithm. Chaotic maps are deterministic systems similar to non-linear systems whose behavior is highly dependent on the initial conditions. The consequence of this behavior is that a small variation of the initial conditions in the transformation map drastically changes the behavior of the system. This feature is extremely exploited in cryptographic protection systems.

C. Generalized Multii-Stage Arnold Transformation - GMSAT

The basic idea of GMSAT consists in the successive application of several different Arnold transformations - stage (I) with its own parameters on the watermark. Transformation parameters of the i-th stage a_i, b_i, and the number of consecutive iterations of the stage k_i represent keys for encryption, while the Arnold transform stage of the T_i stage is additionally required for decryption [5], [12]. In this paper, a generalized multi-stage Arnold transformation - GMSAT is used, in which the variation of the square watermark dimension is permitted in each stage. Thus, at each stage (i) of this transformation, it is possible to choose the arbitrary value of the square watermark to which it is applied, provided that $N_i \leq N$. Each stages of the generalized multi-stage 2D Arnold transformation (i) can be described by the expressions (2) and (3):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & b_i \\ a_i & a_i b_i + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \right) mod N_i \quad (2)$$

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

$$(x, y) \in (0,1, \dots, N_i - 1) \times (0,1, \dots, N_i - 1) \subset Z^2 \quad (3)$$

where x_n, y_n i x_{n+1}, y_{n+1} represent the pixel locations of the 2D watermark before and after transformation respectively. The values of parameters I, a_i, b_i i and N_i represent the parameter set of GMSAT. As with MSAT, the application of GMSAT requires knowledge of the additional parameter T_i [11]. Complete parameters set of *KeyI* determines GMSAT and consists of all I stages parameters union (4):

$$Key_{\mathrm{I}} = \bigcup_{i=1}^{I} E_i(a_i, b_i, k_i, N_i, T_i) \quad (4)$$

where E_i is i-th stage parameter set and operator U (•) represent set union. During scrambling, the original watermark is entered at the entrance of the first stage E_1, while the output of the first stage is brought to the entrance of second stage, and so on. At the entrance of the last stage I, the exit of the last stage I-1 is brought. At the exit of the I-th stage, a scrambled watermark is obtained, which is embedded in all frames. Inverse GMSAT is realized using GMSAT T_i-K_i times.

In addition to adapting watermarks to more convenient forms for inserting, it is also possible to adjust the dimensions of the watermarks.

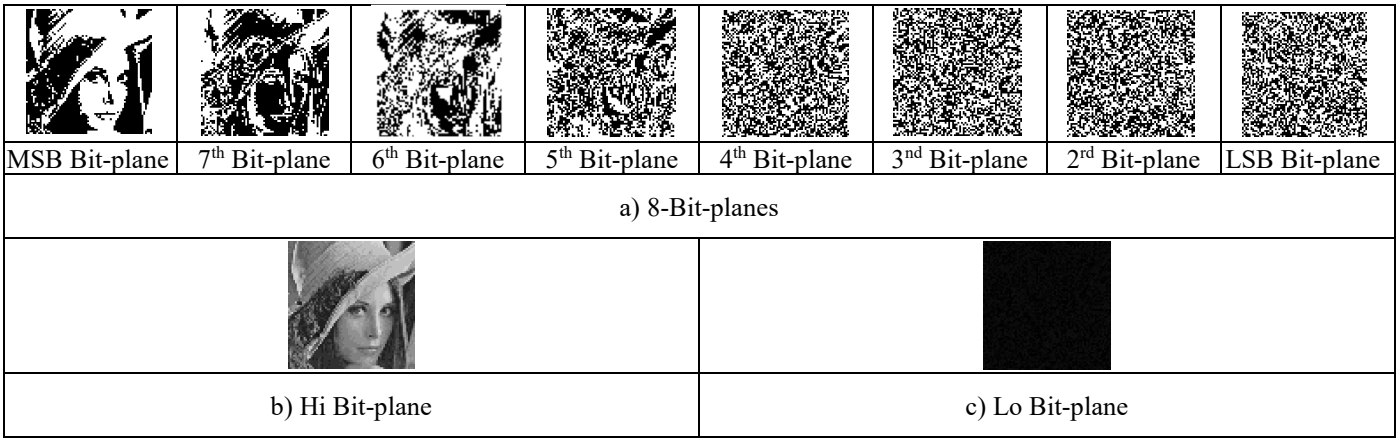


Fig. 2. Decomposition of black-and-white watermark a) 8-bit bit-planes and 4-Bit planes b) Hi Bit plane c) Lo Bit plane

IV. WATERMARK INSERTING IN DWT-SVD-GMSAT DOMEN

In this paper, the insertion and extraction of the watermark in the video frame by a reliable SVD algorithm is performed [14]. The reliable SVD algorithm solves a false positive problem that is inherent in a standard SVD algorithm. The details of the algorithm for embedding the encrypted watermark in the DWT-SVD domain are represented by the sequence of the next steps.

A. Watermark insertion algorithm

Step I1: Decomposition of the **Y** component frame $\boldsymbol{F}$ using second level DWT transformation to obtain $\boldsymbol{F}^k$ i $\boldsymbol{F}^l$ sub-bands:

$$\{\boldsymbol{F}^k, \boldsymbol{F}^l\} = \underset{Haar}{DWT_2}(\boldsymbol{F}) \tag{5}$$

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

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

Step I2: SVD decomposition sub-bands $\boldsymbol{F}^k$:

$$\boldsymbol{F}^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_F^k \cdot (\boldsymbol{V}_F^k)^T . \tag{6}$$

Step I3: Watermark decomposition to *Hi* and *Lo* bit-planes:

$$\boldsymbol{W'}_{\boldsymbol{Hi,Lo}} = \underset{Hi,Lo}{Bit\_plane}(\boldsymbol{W'}) \tag{7}$$

Step I4: Encryption of the decomposed watermarks $\boldsymbol{W'}_{\boldsymbol{Hi,Lo}}$ using GMSAT and obtaining the scrambled watermarks $\boldsymbol{W}_{\boldsymbol{Hi,Lo}}$, which are inserted in each frame.

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

$$i = 1,2,\dots I . \tag{8}$$

Step I5: SVD decomposition of scrambled watermarks $\boldsymbol{W}_{\boldsymbol{Hi,Lo}}$ and calculate the *principal component* $\boldsymbol{A}_{\text{wa}}$.

$$\boldsymbol{W}_{\boldsymbol{Hi,Lo}} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w \cdot \boldsymbol{V}_w^T = \boldsymbol{A}_{wa} \cdot \boldsymbol{V}_w^T ;$$

$$\boldsymbol{A}_{wa} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w . \tag{9}$$

Step I6: Embedding the principal component $\boldsymbol{A}_{\text{wa}}$ in the diagonal matrix of the sub-band $\boldsymbol{S}_F^k$ by the insertion factor α:

$$\boldsymbol{S}_{F\_1}^m = \boldsymbol{S}_F^m + \alpha \cdot \boldsymbol{A}_{wa}. \tag{10}$$

$$m\epsilon\{LL_2, HH_2\}$$

Step I7: Creating a modified sub-bands with an embedded watermark:

$$\boldsymbol{F}_w^m = \boldsymbol{U}_F^m \cdot \boldsymbol{S}_{1\_F}^m \cdot (\boldsymbol{V}_F^m)^T . \tag{11}$$

Step I8: Replacement of the original sub-bands of the second level with modified ones and the application of the inverse discrete wavelet transformation IDWT_2 to obtain a watermarked frame [15].

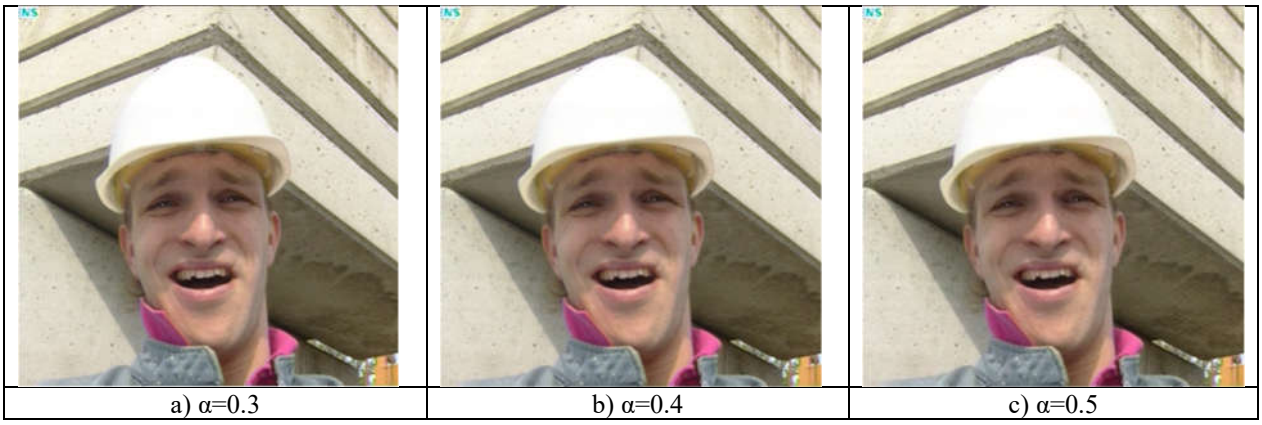
$$\boldsymbol{F}_w = \underset{Haar}{IDWT_2}(\boldsymbol{F}_w^k,\ \boldsymbol{F}^l) . \tag{12}$$

$$i = 1,2,\dots I . \tag{13}$$

The extraction algorithm is inverse to this shown algorithm and is not specifically described in this paper. A similar inverse algorithm can be found in [12].

V. EXPERIMENTAL RESULTS AND ANALYSIS

As the watermark in the experimental part of the work, an adapted central part of the well-known black and white image "*Lena.bmp*" was used in a resolution of 72 × 72 pixels. The appearance of all bit planes are shown in Fig. 2a). In this work, instead of all bit-planes, two 4-bit planes are used for insertion. In this paper, 4-bit planes are called *Hi-bit* and *Lo-bit* planes. The appearance of these 4-bit plains is shown in Fig. 2b) and 2c). In the applied algorithm Hi-bit plane, were shifted 4 bits to the right to lower the coefficient values. In order to increase the level of protection, the content of these watermark bit-planes is scrambled by the GMSAT algorithm prior to insertion. In this paper, 4-stage GMSAT was applied with the following parameters $a = [2, 1, 4, 3]$; $b = [2, 1, 2, 1]$; $N = [72, 60, 50, 72]$; $T = [12, 60, 20, 18]$ and $k = [10, 8, 7, 5]$. Scrambled 4-bit watermarks were embedded in the first 50 frames of the adapted familiar video "Foreman.cif" by the proposed algorithm in the luminance channel with the insertion factor α = 0.5. In the LL_2 component of the DWT transformation of the second level, Hi-Bit plane is inserted, while Lo-Bit plane is embedded in the HH_2 component SVD domains were used for insertion. After inserting these Bit-levels, an inverse SVD and DWT transformation were performed to get a protected frame and video. The appearance of the 30-frame protected video with different insertion factors $\alpha = [0.3\ 0.4\ 0.5]$ is shown in Fig. 3.



a) α=0.3 b) α=0.4 c) α=0.5

Fig. 3. Protected frame #30 of the sequence "Foreman.cif" with the insertion factor a) α = 0.3 b) α = 0.4 and c) α = 0.5.

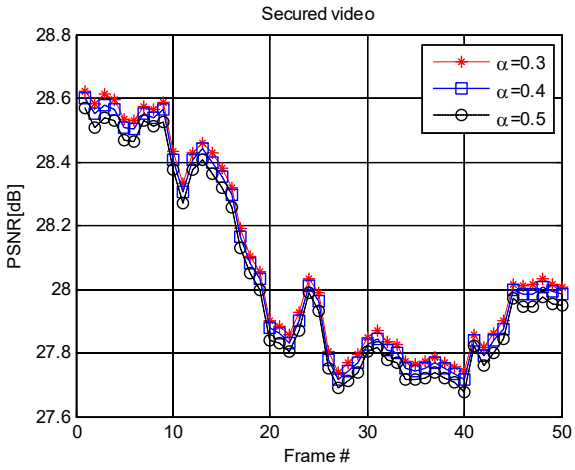


Fig. 4. The quality of protected decoded video in the function of insertion factor for the first 50 frames of the Foreman.cif.

Artefacts in a protected frame are imperceptible, and their influence is shown in Fig. 4 via PSNR. After protection, the video is encoded by H.264/AVC encoder in version 18.4 FRExt. The quality of the extracted trademark was SSIM = 0.7288, while NC = 0.9362. Based on these values, it can be concluded that the extracted watermark can be successfully used to protect the video.

VI. CONCLUSION

Protecting video content is a necessary activity before exposure on the Internet. Inserting a watermark into video content is considerably safer than conventional encryption technologies. The advantage over conventional technologies is in the fact that the watermark protects video content even after playback. In this paper, we have inserted two 4-bit planes into all frame video. Prior to inserting, in order to increase security, these planes were scrambled by the GMSAT algorithm and later inserted into the DWT-SVD domain of each frame. After inserting, the video is encoded by H.264/AVC encoder. On the receiving side, the video is decoded and both 4-bit planes are extracted. The quality of the protected video is very good, while the high quality watermark is extracted at the same time. The results obtained by the simulation are in the ranking with the published, so that the proposed algorithm can be efficiently used to protect video content. The advantage of the proposed algorithm is at the higher level of security it which provides.

LITERATURE

[1] TERA Consultants, "Building a digital economy. The importance of saving jobs in EuropesCreative Economy Paris: International Chamber of commerce, 2010.

[2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–202, Cisco, 2017.

[3] J. Gonzales, "*Mobile First Design with HTML5 and CSS3*", Packt, 2013.

[4] M. Jevtović, Z. Veličković, "Protokoli prepletenih slojeva", Akademska misao, Beograd, 2012.

[5] Z. Veličković, Z. Milivojević, M. Veličković, "Zaštita video sadržaja skremblovanim vodenim žigom pre publikovanja na Intrnetu", YUINFO, pp. 297-302, Kopaonik, 2017.

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

[7] Z. Veličković, Z. Milivojević, M. Veličković, "Digital video protection in the DWT-SVD domain using scrambled watermark by GMSAT algorithm", ETF Jour. of Electrical Engineering, Vol. 23 , pp.36-46, Podgorica, 2017.

[8] K. C. Choi, C. M. Pin, "Robust losless digital watermarking using integer transform with Bit-plane manipulation", Multimed Tools Appl, 75: 21497, 2016, https://doi.org/10.1007/s11042-015-2596-3.

[9] A. M. Joshi, V. Mishra, R. M. Patrikar, "FPGA prototyping of video watermarking for ownership verification based on H.264/AVC", Multimed Tools Appl, 75: 3121-3144, 2015, https://doi.org/10.1007/s11042-014-2426-z.

[10] Z. Tang, J. Song, X. Zhang, R. Sun, "Multiple-image Encryption with Bit-plane Decomposition and Chaotic Maps", Optics and Laserrs Eng. vol. 80, pp. 1-11, 2016, https://doi.org/10.1016/j.optlaseng.2015.12.00

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

[12] Z. Veličković, Z. Milivojević, M. Veličković, „Insertovanje vodenog žiga skremblovanog GMSAT algoritmom u DWT-SWD domenu", INFORMACIONE TEHNOLOGIJE, pp. 221-224, Žabljak 2017.

[13] S. Stanković, I. Orović, E. Sejdić, *Multimedia Signals and Systems*, Spinger, 2012.

[14] C. Jain, S. Arora, P. Panigrahi, "A Reliable SVD based Watermarking Scheme", Journal CoRR, vol. abs/0808.0309, 2008.

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