The Watermark Applications in Multimodal Biometric Identification

Zoran Veličković*, Zoran Milivojević*, Marko Veličković *
* College of Applied Technical Sciences, Niš, Serbia
zoran.velickovic@vtsnis.edu.rs, zoran.milivojevic@vtsnis.edu.rs, marko.velickovic93.rsni@.yahoo.com

***Abstract:*— The need for personal identification in the modern world in all areas of social activity is growing. This paper presents the application of the watermark in multimodal biometric identification. In one biometric feature - a face photo is inserted in the form of a watermark, a second, encrypted biometric feature - a fingerprint. Unlike standard biometric identification algorithms that require access to a database with biometric features, the concept of multimodal biometric identification does not require access to the database. It has been shown that a high quality fingerprint can be extracted from the watermarked photo of person, which, together with the face image, is used in the process of multimodal identification. In the experimental part of the work, mean values of PSNRs of secured images of over 37dB were obtained, while the average value of PSNR watermarks was over 33dB, NC greater than 0.98 and SSIM about 0.96. Based on the obtained experimental results, it can be concluded that the proposed concept of multimodal biometric identification based on a watermark can be successfully applied in multimodal personal identification.**

I. INTRODUCTION

The need for reliable personal identification in the modern world is growing day by day in all areas of social activity. Personal identification is present both in every day routine activities and specialized activities related to security and crime analysis. Classical personal identification is based on identification documents that contain basic person data. Identification through identification documents has become mandatory when crossing the state border, entering government institutions, banks, travel terminals, universities, schools and other public institutions. The information that is standardly used for personal identification is full name, person photo, PIB, ID number, e-mail and telephone number. For applications requiring a higher degree of security, the process of personal identification should include the verification of biometric characteristics [1].

In addition to the physical measures of a person, some specific behavior such as way of walking, keyboard typing or signing method can be used for personal identification. In practice, a biometric personal identification based on DNA, facial shape, arm geometry, palm print, voice characteristics, etc. can be found. Traditionally, fingerprints are used for biometric personal identification, but identification methods using Iris texture are increasingly encountered [2]. Identification of the person through biometric characteristics is based on the comparison of the biometric data of the person from the database with the biometric data collected in the field.

In this paper, the concept of multimodal personal biometric identification is proposed, which involves inserting a scrambled fingerprint into a face photo as a watermark. Inserting the watermark should not cause noticeable degradation of the face image, but at the same time, it should provide its reliable extraction. These are the two contradictory requirements that the insertion algorithms should reconcile. The mathematical apparatus used in this paper for inserting a watermark into the image is based on the DWT (*Discrete Wavelet Transformation*) and SVD (*Singular Value Decomposition*). The safety of the model is further enhanced by scramble the fingerprint by the GMSAT (*Generalized Multistage Arnold Transformation*) algorithm before inserting into the face image. Methods of inserting a watermark are characteristic in copyright protection procedures against the illegal copying and distribution of multimedia content [3]. It has been shown that the watermark - scrambled fingerprint information can be extracted with satisfactory quality in order to be used in the process of personal identification. Unlike classic personal identification where problems can arise when trying to access a remote database, in the proposed concept, fingerprints are extracted on the site and at the time of verification [4].

In addition, one of the problems that can arise is the unknown identity of the persons to identify previously- their data are not in the database. The proposed concept addresses both problems. The idea that the fingerprint is attached and incorporated into a photo of a person brings a series of benefits. Firstly, the proposed system does not require access to a database with stored fingerprint images. This also results in no rights to access the database. The proposed system also solves the problem when the identity of the person is unknown in advance. The proposed concept can also be applied to paper documents, which gives him certain advantages in terms of the necessary financial resources for its realization.

The rest of the work is structured as follows. The second chapter describes generic biometric identification systems and determines the necessary characteristics which they need to possess. Also, this chapter describes how to get a high-quality image of a fingerprint, and describes its basic characteristics.

The third chapter presents the scrambling, inserting, and extraction the watermark from the image used in this paper. The fourth chapter provides details of the proposed algorithms and evaluate the proposed methods.

The obtained results were analyzed on the basis of objective image quality parameters such as PSNR (*Peak Signal-to-Noise Ratio*), NC (*Normalized Correlation*) and SSIM (*Structural SIMilarity*). In the fifth chapter, appropriate conclusions were made on the application of the proposed concept based on the conducted tests.

a) b) c)

Figure 1. Fingerprint scanners a) optical, b) capacitive and c) ultrasound.

II. BIOMETRIC IDENTIFICATION SYSTEMS

The basic function of biometric identification systems is to perform personal identification based on the known biometric characteristics of a person. In general, biometric identification systems can be classified into unimodal and multimodal. In unimodal systems, identification is performed based on one biometric feature, while in multimodal systems identification is performed based on fusion of several biometric features. Biometric multimode systems are safer, more reliable, and more resistant to malicious attempts. In standard biometric identification systems, at least two stages are distinguished. The first step involves the acquisition of biometric data by specialized biometric scanners. Thus, optical, capacitive or ultrasonic fingerprint readers are used for scanning, while microphones are used for recording speech, for scanning the face of the CCD camera, and for reading the iris of the NIR (*Near-Infrared*) cameras. The first stage ends with the digital processing of the collected data to form characteristic features. Specific biometric features obtained in this way, together with personal information are stored in the database. A database of characteristic features and personal information can be found on a local or remote computer. If the database is located on a local computer, the security issue is more complicated, while access to data is simpler and faster. In this case, there may be ethical problems with the right to own a database of biometric features as well as the costs of its protection against unauthorized access [4]. If the database is located on a remote computer, network problems, as well as issues related to access permits, may also be reported. The second stage is a matching phase in which the process of obtaining biometric features on the site is repeated, compared with the features stored in the database. By agreeing biometric data obtained on the site with the one from the base, a personal identity is established. In order for a biometric system to be acceptable for use, it must possess the following characteristics: UNIVERSALITY - the required biometric feature should be owned by all individuals; DISTINCTIVENESS - a biometric feature should be unique to the individual; PERMANENCE - biometric features must be constant over a certain period of time; COLLECTABILLITY - biometric features should be acquired and digitally processed and ACCEPTABILITY - biometric features should be acceptable for users and individuals.

The idea that the fingerprint is incorporated into a photo of a person brings a series of benefits. Firstly, the proposed system does not require access to a database with stored fingerprint features. This also results that there is no need to provide access rights to databases. The proposed system also solves the problem when identity of the person to be identified is unknown earlier. The proposed method has an advantage over others because it can be applied effectively both on electronic and on paper documents.

A. Fingerprint

Fingerprint is a specific feature of a person. This is an image print resulting from the sweating of the papillary lines. Papillary lines appear as a consequence of creases and fissures on human fingers. The unique interaction of the creases and fissures on the finger determines the personal identity. Functionally, the role of the creases is to increase the surface of the skin on the fingers, which increases the number of nerve endings that makes the finger more sensitive. Fingerprints are formed during the embryonic development of a man and are also different in single-skinned twins. Because the fingerprint is a permanent and individual feature of every human being for many years, it is used for personal identification. To collect fingerprints, a whole series of scanners are used that work on different physical principles. On Fig. 1 examples of a) optical, b) capacitive and c) ultrasonic fingerprint scanners are shown.

The examples of the shown scanners are simultaneously performing scanning and digitizing the image of the print. The quality of the prints arrives significantly affects the efficiency of the personal identification algorithms. The degradation of the fingerprint image associated with interruptions of the papillary lines can significantly affect the incorrect determination of the fingerprint. Also, parallel papillary lines can often not be distinguished in the presence of noise in the image of the fingerprint. It is desirable that the resolution of the scanned prints is 500 DPI, while the image size of the image is 300 × 300 pixels. In this paper, fingerprints were used in a resolution of 256 × 256 pixels with 256 gray levels. It is extremely important to extract inserted fingerprints of the highest quality from the stamped photo of the person. The digitized fingerprints used in this paper are shown in the second column of Table 1.

III. ALGORITHMS FOR WATERAK SCRAMBLING, INSERTING AND EXTRACTING

Under the fingerprinting, this paper implies the process of inserting some secret information into multimedia content. In this work, a fingerprint image is a secret information that is inserted into a person's photo. The insertion process should not cause noticeable degradation of the image of a person's face while at the same time allowing an effective extraction of the fingerprints. By inserting a watermark with a higher insertion coefficient α, a more reliable extraction is provided, but at the same time, it causes visible degradation of the image of the face photo

a) Original b) Y component c) C_b component d) C_r component

Figure 2. Decomposition a) original image of "Lena" in b) Y, c) C_r and d) C_b component of the YC_rC_b format

with the inserted watermark. The choice of the insertion coefficient value is very important and depends on many factors. In order to increase safety, the watermark image is scaled by GMSAT (Generalized MultiStage Arnold Transformation) algorithm [3] before insertion. The scrambled watermark is incorporated in this work in the DWT-SVD domain. In this paper, a reliable SVD algorithm was applied which solves the problem of false detection of a trademark that is characteristic of the standard SVD algorithm. Below are the basics of GMSAT and DWT-SVD algorithms [5].

A. GMSAT algorithm for watermark scrambling

In order to scramble the watermark content, the authors proposed in the previous papers the GMSAT (*Generalized Multistage Arnold Transformation*) [3]. The basic idea of this transformation is based on the successive application of several different Arnold transformations - the watermark stage. The transformation parameters of *i*-th transformation a_i, would be the number of consecutive iterations of the stage representing keys for encryption, while the Arnold transformation phase of the T_i stage is additionally required for the application of the inverse GMSAT. The application of GMSAT allows the variation of the square watermark dimension in stages. Each of the stages of the generalized multipack 2D Arnold transformation (i) can be described by the expressions (1) and (2):

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

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

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

where x_n, y_n i x_{n+1}, y_{n+1} represent the locations of the watermark pixel, and a_i , b_i, and N_i represent the Arnold transformation parameters. When using inverse GMSAT, the same procedure is repeated with the same parameters only in reverse order. Details of the DWT-SVD algorithm for insertion and extraction [5] are given below.

B. DWT - SVD algorithm for watermark inserting in cover image

Step $\mathbf{I}_1$: Conversion of face image **F** from RGB Color space to YC_bC_r color space:

$$\{\boldsymbol{Y}, \boldsymbol{C_b}, \boldsymbol{C_r}\} = RGB2YCbCr(\boldsymbol{F}) \quad (3)$$

Step $\mathbf{I}_2$: Decomposition of the **Y** component using a DWT transformation:

$$\{\boldsymbol{Y}^k\} = \underset{Haar}{DWT}(\boldsymbol{Y}) \, , k\epsilon\{LL, HL, LH, HH\} \quad (4)$$

Step $\mathbf{I}_3$: SVD decomposition all of subbands $\boldsymbol{Y}^k$:

$$\boldsymbol{Y}^k = \boldsymbol{U}_Y^k \cdot \boldsymbol{S}_Y^k \cdot (\boldsymbol{V}_Y^k)^T \, . \quad (5)$$

Step $\mathbf{I}_4$: Scrambling the fingerprint image $\boldsymbol{W}$' using the GMSAT algorithm and obtaining a scrambled fingerprint image $\boldsymbol{W}$ that is inserted into the face image.

$$\boldsymbol{W} = \underset{E_i(a_i, b_i, k_i, N_i, T_i)}{Gen\_Arnold}(\boldsymbol{W'}) \quad i = 1,2, \dots I \, . \quad (6)$$

Step $\mathbf{I}_5$: SVD decomposition of scrambled watermark $\boldsymbol{W}$ and calculating the principal component of $\boldsymbol{A}_{wa}$ [5].

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

$$\boldsymbol{A}_{wa} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w \, . \quad (7)$$

Step $\mathbf{I}_6$: Insertion principal component $\boldsymbol{A}_{wa}$ in the diagonal matrix of the subband $\boldsymbol{S}_Y^k$ with the insertion factor α_1 for k$\epsilon\{LL_1, HL_1, LH_1\}$ and α_2 for k$\epsilon\{HH_1\}$:

$$\boldsymbol{S}_{Y\_1}^k = \boldsymbol{S}_Y^k + \alpha_l \cdot \boldsymbol{A}_{wa}, \quad \alpha_l \epsilon \{1, 2\} \quad (8)$$

Step $\boldsymbol{I_7}$: Creating modified subbands with built-in watermark:

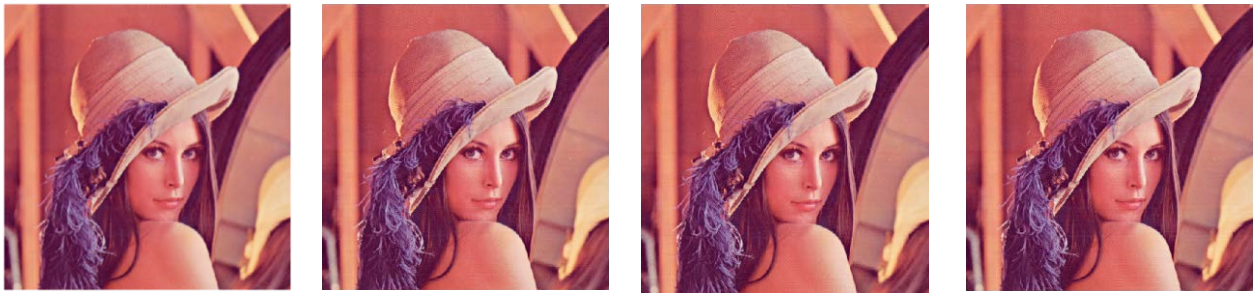
$$\boldsymbol{Y}_w^k = \boldsymbol{U}_Y^k \cdot \boldsymbol{S}_{Y\_1}^k \cdot (\boldsymbol{V}_Y^k)^T \, . \quad (9)$$

Step $\boldsymbol{I_8}$: Replacing the original first-level image subbands with modified and applying an inverse discrete wavelet transform IDWT to obtain a secured image

$$\boldsymbol{Y}_w = \underset{Haar}{IDWT}(\boldsymbol{Y}_w^k) \, . \quad (10)$$

Step $\boldsymbol{I_9}$: Conversion of protected face image from YC_bC_r color space to RGB color space:

$$\{\boldsymbol{F_w}\} = YC_bC_r2RGB(\boldsymbol{Y_w}, \boldsymbol{C_b}, \boldsymbol{C_r}). \quad (11)$$



a) Original b) PSNR = 37.4243 dB c) PSNR = 37.2544 dB d) 36.6933 dB

Figure 3. Appearance a) of the original image, b) and c) watermarked images with the corresponding watermarks from Tab. 1

C. DWT - SVD algorithm for watermark extracting from secured image

The process of extracting the watermark $\boldsymbol{W}^*$ from the protected face image can be done with the following **E** steps:

Step **E**$_1$: Conversion of protected Face image $\boldsymbol{F}_{\boldsymbol{w}}^*$ from RGB color space to YC_bC_r color space:

$$\{\boldsymbol{Y}_{\boldsymbol{w}}^*, \boldsymbol{C}_{\boldsymbol{b}}^*, \boldsymbol{C}_{\boldsymbol{r}}^*\} = RGB2YCbCr(\boldsymbol{F}_{\boldsymbol{w}}^*) \quad (12)$$

Step **E**$_2$: Decomposition $\boldsymbol{Y}_{\boldsymbol{w}}^*$ component using DWT transformation:

$$\{\boldsymbol{Y}_{\boldsymbol{w}}^{*k}\} = \underset{Haar}{DWT}(\boldsymbol{Y}_{\boldsymbol{w}}^*) \ , k\epsilon\{LL, HL, LH, HH\} \quad (13)$$

Step **E**$_3$: SVD decomposition of subbands $\boldsymbol{Y}_{\boldsymbol{w}}^{*\boldsymbol{k}}$:

$$\boldsymbol{Y}_{\boldsymbol{w}}^{*k} = \boldsymbol{U}_{\boldsymbol{Yw}}^{*k} \cdot \boldsymbol{S}_{\boldsymbol{Yw}}^{*k} \cdot \left(\boldsymbol{V}_{\boldsymbol{Yw}}^{*k}\right)^T \quad (14)$$

Step **E**$_4$: Creating the difference between the original ($\boldsymbol{Y}^k$) and the protected face image ($\boldsymbol{Y}_{\boldsymbol{w}}^{*k}$):

$$\boldsymbol{Y}_{\boldsymbol{1}}^{\boldsymbol{k}} = \boldsymbol{Y}_{\boldsymbol{w}}^{*k} - \boldsymbol{Y}^k \quad (15)$$

Step **E**$_5$: Determination of the principal component:

$$\boldsymbol{A}_{\boldsymbol{wa}}^{*k} = \frac{\left(\boldsymbol{U}_{\boldsymbol{Y}}^{\boldsymbol{k}}\right)^{-1} \cdot \boldsymbol{Y}_{\boldsymbol{1}}^{\boldsymbol{k}} \cdot \left(\boldsymbol{V}_{\boldsymbol{Y}}^{\boldsymbol{k}\,T}\right)^{-1}}{\alpha_l}, \ l\epsilon\{1, 2\} \quad (16)$$

Step **E**$_6$: Calculating the inserted scrambled watermark $\boldsymbol{W'^*}$ is performed as follows:

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

Step **E**$_7$: Decrypting the scrambled watermark $\boldsymbol{W}'^{*k}$ using the inverse GMSAT transformation and obtaining the original $\boldsymbol{W}^{*k}$:

$$\boldsymbol{W}^{*k} = \underset{E_i(a_i, b_i, k_i, N_i, T_i)}{Inv\_Gen\_Arnold}(\boldsymbol{W}'^{*k}),$$

$$i = 1,2, \ldots I., \ \ k = HH \quad (18)$$

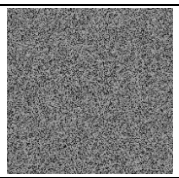
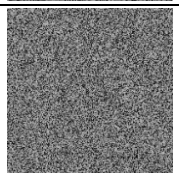
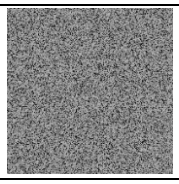
IV. EVALUATION OF THE PROPOSED ALGORITHM

Without compromising the significance of this algorithm, this paper uses an uncompressed **.png* format for storing uncoded face image. This format belongs to the class of RGB color space, while the application of the proposed algorithm requires its transformation into the YC_rC_b color space. Note that in the YC_rC_b format, the information about each image pixel is stored in characteristic matrices marked as Y, C_b, and C_r. In the Y matrix, the values of the brightness for each pixel of the image are stored, while the color information is stored in the C_b and C_r matrices. Inserting a watermark in the transformed domain is performed only in the Y matrix using the DWT-SVD decomposition of this matrix. The proposed algorithm envisages inserting a scrambled watermark in the HH subband of the Y component with an insertion factor $\alpha_2 = 0.05$, while in the other subbands LL, LH, HL, the watermark is inserted by a lower insertion factor $\alpha_1 = 0.0125$.

Figure 3a shows the appearance of the original "Lena" image in a resolution of 512 × 512 pixels, while in Figures 3b and 3c the layouts of the bearing image "Lena" are displayed after inserting the scrambled watermarks shown in Tab. 1. Below the secured figures, the PSNR values obtained after the insertion of the watermarks are displayed. Step I_3 performs SVD decomposition of each subband to prepare for insertion into the SVD domain. Step I_4 scramble the content of the watermark by G4SAT algorithm. The parameters of the applied G4SAT algorithm are shown by the vectors: a = [2 1 4 3], b = [2 1 2 1], T = [128 150 96 192], k = [51 72 83 94] and N = [256 200 186 256]. The content of the parametric vectors is actually the key to the later decompression of the watermark. Tab. 1 shows the prospect of watermarks - fingerprints at a resolution of 256 × 256 pixels used in the practical part of the work. In the first column, the regular numbers of people with displayed fingerprints are shown. The second column contains the original watermarks of the person, while the third column shows the prospects of scrambled watermarks. This scrambled fingerprint image is inserted into the supporting image "Lena" by a reliable SVD algorithm [5], [6].

Steps I5 to I8 refer to inserting a scrambled watermark into all DWT decomposition subbands. In these steps, SVD transformations of all subbands and scrambled watermarks are used for insertion. By changing the S matrix of each subbands, the insertion of the watermark in the cover image is actually carried out. In the last step of I9, the secured image from the YCrCb domain is again transformed into a RGB domain. The Cb and Cr components required for this

TABLE I
ORIGINAL, SCRAMBLED AND EXTRACTED WATERMARKS

Person number	Original watermarks	Scrammbled by G4SAT	Extracted watermarks	PSNR [dB]	NC	SSIM
1				32.9746	0.9932	0.97188
2				33.0093	0.9952	0.97063
3				32.9528	0.9515	0.95153

transformation are taken from the decomposed originals. High PSNR values of 37.42 dB, 37.25 dB and 36.69 dB images show a seamless image degradation. This data clearly indicates that the insertion of the watermark by the proposed algorithm is very good, that is, it does not cause significant visual degradation of the carrier image. This is one of the basic requirements to be satisfied by good insertion algorithms. Another, more important feature to be possessed by these algorithms is the reliable extraction of inserted watermarks of satisfactory quality. The extraction algorithm is based on the inverse process of insertion and is described by the algorithm steps E1 to E7. The obtained results of watermark extraction are below. In order to decrypt the content of watermarks, an inverse G4SAT algorithm must be applied [3], [5]. The fourth, fifth and sixth columns of Tab. 1 show the results obtained for all three used watermarks. For the evaluation of the quality of extracted watermarks, objective parameters of image quality assessment were used: PSNR, NC and SSIM coefficients [7]

The quality of the extracted watermarks that represent the image of the fingerprint texture is about 33dB, which is extremely good. The quality of the carrier image is higher than 37 dB, which is also considered a very good result. The quality of the extracted mark expressed by averaged normalized cross-correlation NC is about 0.99, and over SSIM about 0.96 that is considered a good result [8].

V. CONCLUSION

Personal identification based on identification documents is present in all areas of human activity from access control to cash transactions. When a higher degree of security is required, identification methods that check the person's biometric features are used . In this paper, a watermark-based model was developed for the needs of biometric personal identification. A scrambled image of a fingerprint is inserted as a watermark in another biometric feature - a photo of a person's face. When watermark was inserted in the carrier image, there is no visible degradation of quality. On the other hand, the shown method provides extraction of the high quality fingerprint so that it can be used in the personal identification process. In the process of multimodal identification, the face of the person is compared with photographs on the identification documents, also, the extracted fingerprint with a scanned fingerprint on the site is compared. The obtained results justify the use of this method in the processes of "off-line" multimodal personal identification.

REFERENCES

[1] Lumini, A., Nanni, L., Overview of the combination of biometric matchers, Infmation Fusion, Vol. 33, pp. 71–85, 2017.

[2] Miao D. M., Zhang, Z. Sun, T. Tan, Z., He, Bin-based classifier fusion of iris and face biometrics, Neurocomputing, Vol. 224, pp. 105-118, 2017.

[3] Veličković, Z., Blagojević, D., Milivojević, Z., Veličković, M., Poboljšanje bezbednosti skremblovanog vodenog žiga u haos domenu, INFOFEST, pp. 174-182, 2016.

[4] Elazhary, H., A Framework for Offline Biometric Identity Authentication, Int. Jour. Comp. Sci. and Inform. Security - IJCSIS, Vol. 12, No. 12, 2014.

[5] Veličković, Z., Milivojević, Z., Veličković, M., „Insertovanje vodenog žiga skremblovanog GMSAT algoritmom u DWT-SWD domenu“, Informacione tehnologije, pp. 221-224, Žabljak 2017.

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

[7] Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P., Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE Trans. on Image. Proc., Vol. 13, No. 4, 2004.

[8] Veličković, Z., Milivojević, Z., Veličković, M., “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.