UDC 004.932 **doi:** https://doi.org/10.20998/2522-9052.2021.3.15

Igor Ruban, Nataliia Bolohova, Vitalii Martovitskyi, Roman Yaroshevych

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF METHODS FOR EMBEDDING DIGITAL WATERMARKS

Abstract. In recent years, we have seen a significant increase in traffic moving across various networks and channels. The development of technology and global network leads to an increase in the amount of multimedia traffic. To authenticate and avoid abuse, data should be protected with watermarks. This paper discusses various robust and invisible watermarking methods in the spatial domain and the transform domain. The basic concepts of digital watermarks, important characteristics and areas of application of watermarks are considered in detail. The paper also presents the most important criteria for assessing the digital watermark effectiveness. Based on the analysis of the current state of the digital watermarking methods, robustness, imperceptibility, security and payload have been determined as the main factors in most scientific works. Moreover, researchers use different methods to improve / balance these factors to create an effective watermarking system. Our research identified the main factors and new techniques used in modern research. And the assessment of watermark method effectiveness was proposed.

Keywords: digital watermark; authentication; LSB; copyright protection; digital image; steganographic; cyber-security.

Introduction

In recent years, we have seen a significant increase in traffic moving across various networks and channels. The development of technology and global network leads to an increase in the amount of multimedia traffic [1]. To authenticate and avoid abuse, data should be protected with watermarks. A digital watermark prevents illegal copying and distribution of multimedia content by hiding unremarkable ownership data [2, 3]. A digital watermark (DWm) is a technology used in information security to solve the problem of copyright protection for certain digital in-formation. With this, a special mark is applied to the digital graphic images, which can remain visible or invisible to a person.

The watermark embedding process can be determined based on domain and different groups. According to the domain, the methods of embedding digital water-marks could be divided both in the domain space and during domain transformation, for example, methods based on SVD [4]. Initially, approaches to the spatial domain, in which the process of embedding watermarks can be carried out by directly changing the pixels in an image, were used. It has such advantages as low computational complexity and ease of implementation. The most commonly used techniques in this area are the least significant bit (LSB) and the spread spectrum and correlation. However, techniques such as discrete cosine transforms (DCT), discrete wavelet transforms (DWT), discrete Fourier transforms (DFT), singular value decomposition (SVD), and Karhunen-Loew transforms (KLT) are examples of transform domain techniques. In the context of DWM visibility, there are two different categories of digital watermark: visible and invisible. In addition, there are various types of invisible watermarks that are both robust and fragile. A complete classification of digital watermarks is presented in [4].

Embedding and extracting watermark process

The system for embedding and extracting watermarks is shown in Fig. 1; it performs the tasks of embedding and extracting a digital watermark from a container image. A precoder is a device designed to convert a hidden watermark to a form suitable for embedding in a container. Digital watermark embedding device is intended for embedding a hidden digital watermark in the container image. The system combines two types of information so that they can be seen by two fundamentally different detectors. One of the detectors is a digital watermark extraction system, and another is a human. Pre-processing is often performed using a key to improve the secrecy of the data that is embedded. The following stage is the digital watermark "embedding" into the container, for example, by modifying the least significant bits of the coefficients. This process is possible due to the peculiarities of the human perception system. It is well known that images have great psycho-visual redundancy. The human eye is similar to a low-pass filter that skips fine details [6].

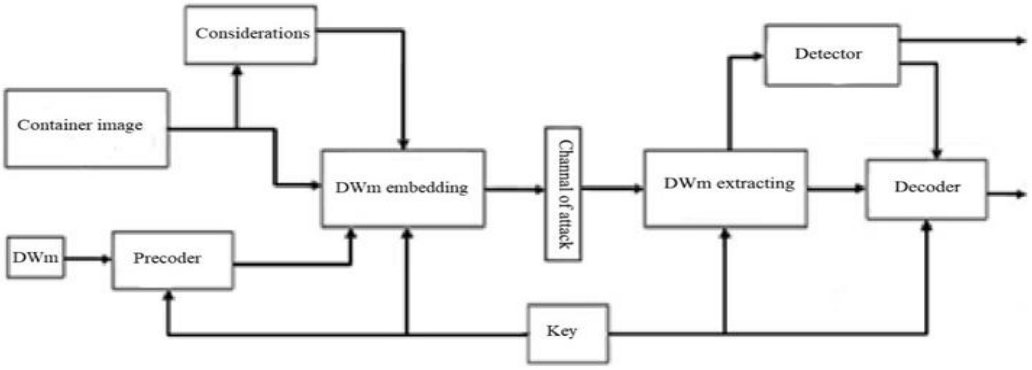

Fig. 1. Embedding and extracting watermark process

Types of digital watermark systems

There are three different types of digital watermarks, which depend on the characteristics and method of their detection [7-9]. A brief description of this system is discussed below (Fig. 2):

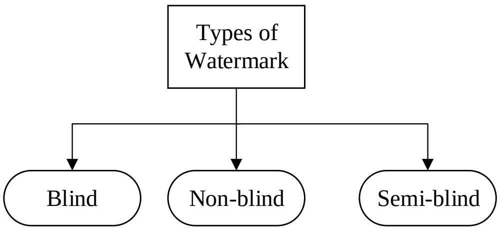

Fig. 2. Main types of watermarks

- Blind Digital Watermarking Method: In this type of system, watermarking only requires a watermarked image, and an original image is not necessary to extract a digital watermark. Potential applications for blind watermarking are healthcare, copyright protection, electronic voting system, and the like.

- Non-Blind Digital Watermarking Method: In such a system, an original image and an embedded image are copied; the watermark and the original image are required to extract the digital watermark. Potential applications for this type of watermarking system are covert communication and copyright protection.

- Semi-Blind Digital Watermarking Method: It works like a non-blind system, requiring additional input. Some important applications for such a system are image authentication, CAD models and the like.

Characteristics of watermark

There are many important properties that characterize the watermark, which are very important for digital watermarking systems [9]. Fig. 3 shows the main characteristics of watermarks.

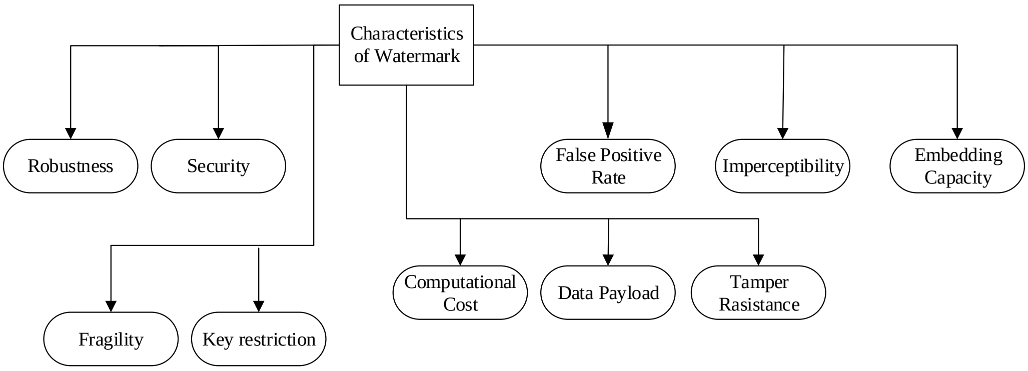

Fig. 3. Characteristics of watermark

Watermark robustness is the ability of an algorithm to resist against noise. Security means the watermark is difficult to change or remove without destroying the container image. Embedding capacity of the watermark is expressed as the amount of information contained in the container. Imperceptibility of the watermark is achieved by invisible to the human eye or ear file modifying. Watermark is called fragile if it cannot be detected with the slightest modification. Such digital watermarks are commonly used for integrity checking. Key restrictions are considered as another characteristic, it is the level of restriction that applies to the readability of the watermark.

Computational cost is described as the total resource cost of embedding and extracting the watermark. Other important characteristics are clearly defined in [10].

Applications of watermarking

Potential researchers use different watermarking schemes for different areas of human activity. These include copyright protection, digital forensics, military affairs, healthcare, medical programs, etc. Some applications are shown in Fig. 4.

1. Copyright protection. The main goal is to protect digital information copyrights by hiding classified information.

2. Broadcast monitoring. It allows content owners to automatically check, when, where and how long content broadcast via cable and satellite television.

3. Digital forensics. This is the process by which the watermarked container contains the recipient's identifier in order to trace the sources of illegal distribution.

4. Application in medicine. Application of reversible digital watermarks for medical image verification.

5. Electronic voting system. An electronic voting system is the process of accompanying elections by maintaining security during elections. Due to the widespread use of the Internet in any industry, such as banking, shopping, filing a tax return, a secure transaction is essential. Obviously, this is an alternative solution for holding elections, given the security of the election process. The most valuable solution to all these problems can be achieved by digital watermark embedding.

6. Distance education. Due to the unavailability of teachers and other problems, distance education is becoming an increasingly powerful method of providing education. Distance learning requires a strong demand for smart technology for the development of distance education. It uses a watermark to ensure the authenticity of data transmission in distance learning, as well as to protect multimedia content [10].

7. Chip and hardware protection: Mohanty et al. [12] introduced the role of watermarks in hardware protection. Intellectual Property (IP) core and hardware protection is a multi-faceted problem comprising of Trojan Security, buyer's ownership security, antipiracy protection. Digital watermarks can be embedded in a layered hardware design

abstraction based on the designer's choice.

8. Cloud data protection. Content-based image search is considered with the increasing number of images in daily life. Images take up more space than text files. Thus, cloud storage can be used to store images. Some sensitive images, such as medical and non-medical images, must be authenticated before being transferred to another location. Cloud server inserts a unique watermark into encrypted images before sending the images to the user. Upon detection of an illegal image, an unauthorized user can be found by the watermark extraction method [13].

Based on the analysis of the areas of application and criteria of the digital watermark, Table 1 presents the important characteristics of the digital watermark (Table 1).

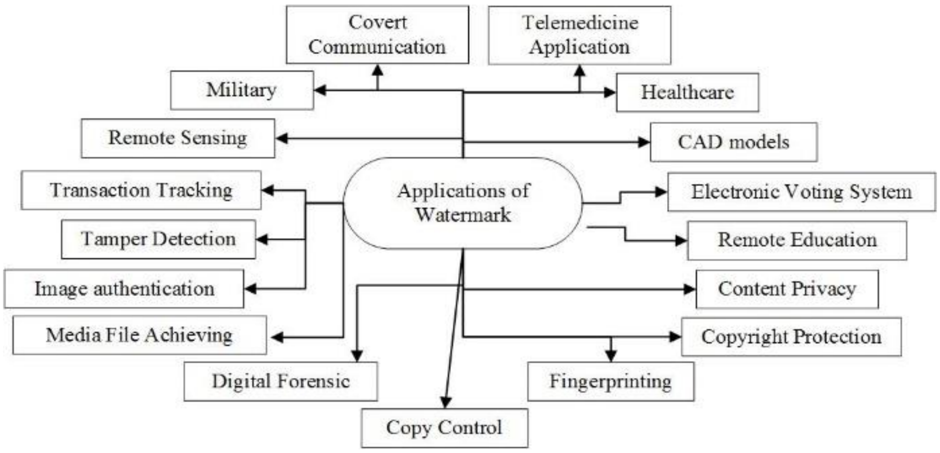

Fig. 4. Watermarking

Table 1 - **Specific uses of watermarks according to their characteristics**

Characteristics	**Definition**
Robustness	Ability of the algorithm to resist attacks
Imperceptibility	As a result of embedding a digital watermark, the image should have a minimum deviation from the original image
False positive digital watermark extracting	Error extracting digital watermark from empty container
Fragility	Digital watermark changes with the slightest modification of the container
Tamper resistance	Ability to resist deliberate attacks
Embedding capacity	Determined by the number of watermarks embedded in the data

Watermark attacks

Task of embedding and extracting information from the container is performed by the stegosystem, which consists of a stegosystem encoder and a stegosystem decoder. Encoder transforms the hidden message into a form suitable for embedding into the signal-container and embeds the hidden message into the signal-container taking into account the model. Decoder detects the presence of a hidden message in the container and, if present, retrieves and recovers the hidden message.

Steganography and cryptography are closely related, but these sciences have different approaches to information security. In particular, cryptography hides information by encryption operation, that is, it is known in advance that the cryptogram contains encrypted information. In turn, steganography hides the fact of the presence of secret information, so the filled container should not differ from the original one. Methods of cryptography and steganography can be combined to increase the security of information.

Stegosystem forms a stegochannel through which the filled container is transmitted. Violators may gain access to this channel. We will briefly describe the harm that violators can cause. For a secret message exchange, two addressees must have a secret key known to both, which determines the location of the hidden message. First of all, a violator can establish the presence of a stegochannel and read messages. Ability to read a message is determined by robustness of the hiding system used. Such type of violators is considered passive.

There is also an active violator who can delete or destroy hidden messages. Although the fact of the interference may be known, the goal of the violator - hacking the stegosystem - may be achieved. The most dangerous is a malicious violator who can substitute stego messages in addition to destroying. Violators use the following attacks to implement threats:

- Active attacks. In this type of attack, the hacker deliberately tries to remove the watermark or simply it undetectable. They are aimed at distorting the embedded watermark beyond recognition.

- Passive attacks. The hackers are trying to determine if there is a watermark, without any destruction or removal. These types of attacks are important in covert communication.

- Counterfeiting attacks. The hackers do not remove the watermark but insert a new valid watermark.

- Collusion attacks. This attack is no different from active attacks. The hacker uses several copies of the same information, each with a different mark, to create a copy from a copy without digital watermark.

- Simple attacks. Another name for this attack is waveform attack and noise attack. These are called simple attacks because the violator tries to harm the embedded watermark by modifying the entire watermark. Examples of these attacks are filtering, noise addition, signal-based compression (JPEG, MPEG), and gamma correction.

- Ambiguity attack. These attacks try to obfuscate by creating fake watermarked data or fake original data. The inversion attack is an example of this type of attack.

- Cryptographic attacks. The main purpose of this attack is to break the security method in watermarking techniques and find a way to remove the inserted watermark information. Due to the high computational cost, the use of these attacks is limited.

- Removal attack. Complete removal of watermark data from information in the container without violating the security of the watermark.

- Geometrical attack. Compared to the removal attacks, these attacks do not actually remove inserted watermark, but change the synchronization of the watermark detector with the inserted information.

Analysis of modern methods of digital watermarking

The analysis performed makes it possible to identify various reliable watermarking approaches to protect confidential information in different areas.

A reliable color image watermarking technique using decision tree induction in the DCT domain has been developed [14]. The method firstly uses DCT to transform the container and watermark image and uses the decision tree induction method to hide the secret watermark.

Paper [15] presents a robust multi-bit image watermarking scheme to render conventional image processing attacks ineffective as well as affine distortion. This scheme combines contrast modulation and efficient synchronization for large payloads and high robustness. The effectiveness and advantages of the proposed scheme are confirmed by experimental results that show superior performance compared to several modern watermarking methods.

The authors have developed a watermarking algorithm using SVD and a genetic algorithm [4, 16]. The method uses a singular vector to insert watermark into the container. In addition, the GA technique is used to improve the efficiency of the proposed scheme.

Wavelet-based watermarking is presented in [17]. The method uses a scale factor to modify a single vector of the container image and watermark. In addition, Multi-Purpose Particle Swarm Optimization (MOPSO) is applied to optimize the balance between conflicting watermarking factors.

The authors developed a watermarking scheme using association rules and vector quantization. First, rules are defined on both 2D barcode and watermark information. In the process of embedding, the defined rules of information about the watermark are embedded into the association rules of information about the container barcode. The results showed that the scheme is safe and has remarkable inlineability [18].

Reversible high capacity watermarking technique using a rhombus pattern, sorting, and histogram shift method was proposed in [19]. First, the container is split into two different datasets and the payload information is embedded in both datasets. The proposed method is reliable and invisible for various attacks.

In [20], the authors developed a pixel-based approach to data hiding. The method uses noise in the image to hide the watermark data. Look-up tables are used to quickly recover hidden watermarks.

In [21], the author proposed a perturbed method for authenticating secret data in the original data and reversing the perturbed data back to the original data. The method uses an adjustable weighting mechanism to estimate the degree of error in the input data. The demonstrated results clearly show that the method is reliable and safe with a large payload volume.

The author developed a robust watermark based on DWT, all phases of the discrete cosine orthogonal transform (APDCBT) and SVD [22]. The container image is transformed by DWT, and two similar watermarks are embedded to the selected areas. Due to the excellent energy concentration, the author applies APDCBT to provide better protection of classified data (watermarks). In addition, imperceptibility is improved by using constant energy ratios.

Fig. 5 shows various effective schemes / solutions to improve robustness of watermarking techniques.

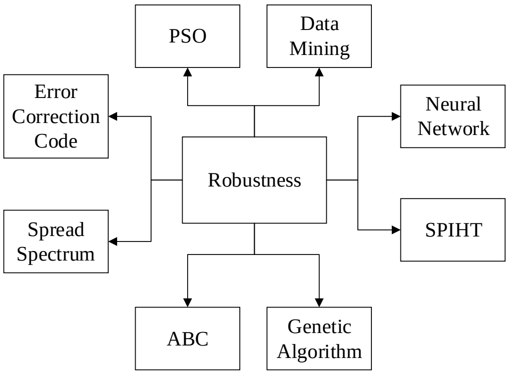

Fig. 5. Identified methods used to increase robustness of watermarking

After analysing the current state of research on watermark methods and significant watermark characteristics, it is possible to form the following assessment of watermark method effectiveness:

$$\begin{aligned} EF = R \cdot \alpha_r + SR \cdot \alpha_{sr} + \\ + ER \cdot \alpha_{er} + SC \cdot \alpha_{sc} + DT \cdot \alpha_{dt}, \end{aligned} \tag{1}$$

where $R, R \in [0,1]$ – a security assessment of the method for digital watermark embedding;

$RS, RS \in [0,1]$ – an assessment of digital watermark invisibility on an image;

$ER, ER \in [0,1]$ – the probability of an error of the first and second kind;

$SC, SC \in [0,1]$ – an assessment of digital watermark fragility;

DT – is the number of embedded digital watermarks;

$\alpha_r, \alpha_{sr}, \alpha_{er}, \alpha_{sc}, \alpha_{dt}$ – significance coefficients of the corresponding criteria of the digital watermark method.

Such coefficients are needed, since there is no universal method for digital watermark embedding, therefore, due to such coefficients, it is possible to adjust the significance of each criteria and thereby influence the final method efficiency for a specific task facing a digital watermark.

As an example, we describe the effectiveness criteria of the digital watermark method for images.

Robustness of the method for digital watermarking can be clarified in a statistical sense by accepting the following assumptions:

The digital watermark method W can be defined as a set of some functions F and G that describe the process of embedding and extracting a digital watermark on a multiple data, such that each element is a pattern required for the digital watermark method:

$$E = (E_i, i = 1, 2, ..., N). \tag{2}$$

For simplicity, we will assume that the input data set includes a pair of values for a container image Im and a digital watermark Wm :

$$E_i = \{\mathrm{Im}_i, Wm_i\}. \tag{3}$$

The method has two stages, embedding $F(E_i) = \mathrm{Im}_i^*$ and extracting $G(\mathrm{Im}_i^*) = Wm_i$. Since robustness is the algorithm ability to resist attacks, we add an attack function $At_j \in At$, where At is the set of admissible attacks on the digital watermark.

$$At = (At_j, j = 1, 2, ..., M)\,. \tag{4}$$

Using the function $At_j(\mathrm{Im}_i^*) = \mathrm{Im}_i^{*\prime}$ will distort the digital watermark container. Then, for some values of E_i the obtained value from $G(\mathrm{Im}_i^{*\prime})$ may be within acceptable limits Δi :

$$\left|G(\mathrm{Im}_i^{*\prime}) - G(\mathrm{Im}_i^*)\right| \leq \vartriangle i\,. \tag{5}$$

For all other E_i, that form subset of $E_l \in E$, execution of $G(\mathrm{Im}_i^{*\prime})$ does not provide an acceptable result, that is:

$$\left|G(\mathrm{Im}_i^{*\prime}) - G(\mathrm{Im}_i^*)\right| > \vartriangle i\,. \tag{6}$$

All such cases are called false.

Each value of E_i represents a possible combination of values that can be input to functions F and G. Number N of possible E is very large, but finite. Combination of actions,

$$F \to \forall At_j, At_j \in At \to\ G, \tag{7}$$

that results in correct reading of the digital watermark from the container or a false positive.

Thus, the probability P that, after an attack on the container with digital watermark $At_j(\mathrm{Im}_i^*) = \mathrm{Im}_i^{*\prime}$ removing the digital watermark from the container will lead to an erroneous result (6) is equal to the probability that the set of input data E_i used in the j attack belongs to the set E_l. Suppose that $n_{l,j}$ is the number of different input data sets contained in E_l for the j attack, then $Q_j = n_{l,j} / N$ is a probability that the execution of the sequence of functions (7) on the data set E_i, randomly selected from E among the equally probable, will result in false digital watermark extraction. In this case, $P_j = 1 - Q_j = 1 - n_{l,j} / N$ is the probability that in the j attack on the input set E_i, randomly selected from E will lead to the correct digital watermark extraction, equation (5). Since various attacks are independent events, the probability that all attacks will not lead to false extraction of the digital watermark, equation (6), is equal to the product probability of each attack:

$$R = \prod_{1}^{j} P_j\,. \tag{8}$$

Robustness of the digital watermark method will be assessed by this product probability.

To assess imperceptibility, it is possible to use various metrics to estimate the difference between two images, such as the signal-to-noise metric. But such a metric will be of a higher order than all other terms, which can lead to a false assessment of the method effectiveness. Therefore, the following metric was proposed for assessing imperceptibility:

$$\begin{gathered}
SR = \frac{h_x + h_y}{2};\\
h_x = \frac{1}{Wh} \times\\
\times \sum_{i=1}^{Wh-1} \left[\frac{1}{\sigma_x^{i-1} \bullet \sigma_x^{i-1}} \cdot \sum_{j=0}^{Ht-1} \begin{matrix} (Di_{i-1,j} - m_x^{i-1}) \times \\ \times (Di_{i,j} - m_x^i) \end{matrix} \right]^2;\\
h_y = \frac{1}{Ht} \times\\
\times \sum_{i=1}^{Ht-1} \left[\frac{1}{\sigma_x^{i-1} \bullet \sigma_x^{i-1}} \bullet \sum_{j=0}^{Wh-1} \begin{matrix} (Di_{i,j-1} - m_y^{i-1}) \times \\ \times (Di_{i,j} - m_y^i) \end{matrix} \right]^2;\\
Di_{x,y} = \left| Y(Pixel'_{x,y}) - Y(Pixel_{x,y}) \right|;\\
m_x^i = \frac{1}{Ht} \bullet \sum_{i=0}^{Ht-1} Di_{i,j};\\
m_y^i = \frac{1}{Wh} \bullet \sum_{i=0}^{Wh-1} Di_{i,j};\\
\sigma_x^i = \sqrt{\sum_{i=0}^{Ht-1} (Di_{i,j} - m_x^i)^2};\\
\sigma_y^i = \sqrt{\sum_{i=0}^{Wh-1} (Di_{i,j} - m_y^i)^2},
\end{gathered} \tag{9}$$

where SR - an indicator for estimating the changes made when embedding digital watermark distortions;

h_x, h_y - average value of the square of linear correlation coefficient of the changes made when embedding digital watermark image distortions vertically and horizontally, respectively;

m_x^i, m_y^i - mathematical expectation of the distortion amount in corresponding column or row of the pixel matrix;

σ_x^i, σ_y^i - standard deviation of the distortion amount in corresponding column or row of the pixel matrix;

$Di_{x,y}$ - amount of brightness distortion in the corresponding pixel;

Wh - image width in pixels;

Ht - image height in pixels;

$Pixel'$ - pixel matrix of the watermarked image;

$Pixel$ - pixel matrix of the original image;

Y - pixel brightness determination operator;

ER - sum of errors of first and second kind when digital watermark extracting from the container.

To assess the fragility of a digital watermark, the following equations will be used.

Suppose that there is some distortion function

$$H(k, imige),$$

where k is the number of distortion pixels, and $imige$ - is an image with an embedded digital watermark. Then the fragility estimate will be as follows:

$$\begin{gathered} F(E_i) = \mathrm{Im}_i^*; G(\mathrm{Im}_i^*) = Wm_i; H(k, \mathrm{Im}_i^*) = \mathrm{Im}_i'^* \\ G(\mathrm{Im}_i'^*) = Wm_i'; \quad SC = count / (W \bullet H); \\ count = \sum_{x=0}^{W} \sum_{y=0}^{H} \begin{cases} 1, if\ Wm'_{i\,[x,y]} \neq Wm_{i\,[x,y]}; \\ 0, if\ Wm'_{i\,[x,y]} = Wm_{i\,[x,y]}, \end{cases} \end{gathered} \qquad (10)$$

where $count$ - number of digital watermark pixels that do not match the original digital watermark after distorting the k pixels of the digital watermark container. W, H - image width and height in pixels.

Conclusion

This paper discusses various robust and invisible watermarking methods in the spatial domain and the transform domain. The basic concepts of digital watermarks, important characteristics and areas of application of watermarks are considered in detail.

The paper also presents the most important criteria for assessing the digital watermark effectiveness. Based on the analysis of the current state of the digital watermarking methods, robustness, imperceptibility, security and payload have been determined as the main factors in most scientific works. Moreover, researchers use different methods to improve / balance these factors to create an effective watermarking system. Our research identified the main factors and new techniques used in modern research. And the assessment of watermark method effectiveness was proposed.

References

1. Merlac, V., Smatkov, S., Kuchuk, N. and Nechausov, A. (2018), "Resourses Distribution Method of University e-learning on the Hypercovergent platform", *Conf. Proc. of 2018 IEEE 9th Int. Conf. on Dependable Systems, Service and Technologies*, DESSERT'2018, Kyiv, May 24-27, 2018, pp. 136-140, DOI: http://dx.doi.org/10.1109/DESSERT.2018.8409114.
2. Van Schyndel, R. G., Tirke,l A. Z. and Osborne, C. F. (1994), "A digital watermark //Proceedings of 1st international conference on image processing" *IEEE*, Vol. 2, pp. 86-90.
3. Islam, M. and Laskar, R. H. (2018), "Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM", *Multimedia Tools and Applications*, Vol. 11, pp. 14407-14434.
4. Loukhaoukha, K. (2012), "On the security of digital watermarking scheme based on SVD and tiny-GA", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 3, no 2. – C. 135-141.
5. Singh, A.K. (2017), "Improved Hybrid Algorithm for Robust and Imperceptible Multiple Watermarking using Digital Images", *Multimedia Tools Applications*, Springer, Vol. 76(6), pp. 881–890.
6. Ruban, I., Bolohova, N., Martovytskyi, V., Lukova-Chuiko, N. and Lebediev, V. (2020), "Method of sustainable detection of augmented reality markers by changing deconvolution", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9(2), pp. 1113-1120.
7. Mun, S. M. (2019), "Finding robust domain from attacks: A learning framework for blind watermarking", Neurocomputing, Vol. 337, pp. 191-202.
8. Roy, A., Maiti, A. K. and Ghosh, K. (2018), "An HVS inspired robust non-blind watermarking scheme in YCbCr color space", *International Journal of Image and Graphics*, Vol. 18, no. 03, DOI: https://doi.org/10.1142/S0219467818500158.
9. Vaidya, P. and PVSSR, C. M. (2017), "A robust semi-blind watermarking for color images based on multiple decompositions", *Multimedia Tools and Applications*, Vol. 76, no. 24, pp. 256.23-256.56.
10. Ruban, I., Khudov, H., Makoveychuk, O., Khudov, V. and Lishchenko, V. (2020), "The Model and the Method for Forming a Mosaic Sustainable Marker of Augmented Reality", *Proceedings - 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, TCSET, pp. 402-406.
11. Singh, A.K., Kumar, B., Singh, G. and Mohan, A (2017), *Medical image watermarking: techniques and applications*, Book series on Multimedia Systems and Applications, Springer, ISBN: 978-3319576985.
12. Mohanty, S.P., Sengupta, A., Guturu, P. and Kougianos, E. (2017), "Everything you want to know about watermarking: From Paper marks to hardware protection", *IEEE Consumer Electronics Magazine*, Vol. 6(3), pp. 83–91.
13. Kuchuk, H., Kovalenko, A., Ibrahim, B.F. and Ruban, I. (2019), "Adaptive compression method for video information", *International Journal of Advanced Trends in Computer Science and Engineering*, pp. 66-69, DOI: http://dx.doi.org/10.30534/ijatcse/2019/1181.22019.
14. Moosazadeh, M. and Ekbatanifard, G. (2016), "Robust image watermarking algorithm using DCT coefficients relation in YCoCg-R color space", *2016 Eighth Int. Conference on Information and Knowledge Technology* (IKT), IEEE, pp. 263-267.
15. Zhong, X. and Shih, F. Y. (2019), "Robust Multibit Image Watermarking Based on Contrast Modulation and Affine Rectification", *Int. J. of Pattern Recognition and Artificial Int.*, Vol. 33, no. 14. https://doi.org/10.1142/S0218001419540363.

16. Paikaray, D. and Mustafi, A. (2020), "Genetic Algorithm-Based Image Watermarking Using Multiple Location", Proc. of the Fourth Int. Conference on Microelectronics, *Computing and Communication Systems*, Springer, Singapore, pp. 617-627.
17. Loukhaoukha, K., Nabti, M. and Zebbiche, K. (2014), "A Robust SVD- based Image Watermarking Using a MultiObjective Particle Swarm Optimization", *Opto-Electronics Review*, Vol. 22(1), pp. 45–54.
18. Shen, J.J. and Hsu, P.W. (2008), "A Fragile Associative Watermarking on 2D Barcode for Data Authentication", *International Journal of Network Security*, Vol. 7(3), pp. 301–309.
19. Sachnev, V., Kim, H.J., Nam, J., Suresh, S. and Shi, Y.Q. (2009), "Reversible Watermarking Algorithm Using Sorting and Prediction", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19(7), pp. 989–999.
20. Pei, S.C. and Guo, J.M. (2003), "Hybrid Pixel-Based Data Hiding and Block-Based Watermarking for Error-Diffused Halftone Images", *IEEE transactions on Circuits and Systems for Video Technology*, Vol. 13(8), pp. 867–884.
21. Lin, CY (2006), "A Reversible Data Transform Algorithm Using Integer Transform for Privacy Preserving Data Mining", *The Journal of Systems & Software*, Vol. 117(7), pp. 104–112.
22. Zhou, X., Zhang, H. and Wang, C (2018), "A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD", *Symmetry MDPI*, Vol. 10(3), pp. 1–15.

Received (Надійшла) 28.05.2021
Accepted for publication (Прийнята до друку) 18.08.2021

About the authors / Відомості про авторів

Рубан Ігор Вікторович – доктор технічних наук, професор, перший проректор, Харківський національний університет радіоелектроніки, Харків, Україна;
Igor Ruban – Doctor of Technical Sciences, Professor, The first vice-rector, Kharkiv National University of RadioElectronics, Kharkiv, Ukraine;
e-mail: ihor.ruban@nure.ua; ORCID ID: http://orcid.org/0000-0002-4738-3286.

Бологова Наталія Миколаївна – аспірантка, Харківський національний університет радіоелектроніки, Харків, Україна;
Nataliia Bolohova – postgraduate, Kharkiv National University of RadioElectronics, Kharkiv, Ukraine;
e-mail: nataliia.bolohova@nure.ua; ORCID ID: http://orcid.org/0000-0001-8927-0055.

Мартовицький Віталій Олександрович – кандидат технічних наук, доцент, доцент кафедри ЕОМ, Харківський національний університет радіоелектроніки, Харків, Україна;
Vitalii Martovytskyi – Candidate of Technical Sciences, Associate professor, Associate professor of Computer Science departments, Kharkiv National University of RadioElectronics, Kharkiv, Ukraine;
e-mail: vitalii.martovytskyi@nure.ua; ORCID ID: http://orcid.org/0000-0003-2349-0578.

Ярошевич Роман Олександрович – асистент, Харківський національний університет радіоелектроніки, Харків, Україна;
Roman Yaroshevych – assistant, Kharkiv National University of RadioElectronics, Kharkiv, Ukraine;
e-mail: roman.yaroshevych@nure.ua; ORCID ID: http://orcid.org/0000-0002-7949-1513.

Методологія оцінки ефективності методів вбудови цифрових водяних знаків

І. В. Рубан, Н. М. Бологова, В. О. Мартовицький, Р. О. Ярошевич

Анотація. В останні роки ми спостерігаємо значне збільшення трафіку, що рухається через різні мережі та канали. Розвиток технологій та глобальної мережі призводить до збільшення обсягу мультимедійного трафіку. Для автентифікації та уникнення зловживань дані повинні бути захищені водяними знаками. У даній роботі розглянуто різні надійні та непомітні методи водяних знаків у просторовій області та області перетворень. Детально розглянуті основні поняття цифрових водяних знаків, важливі характеристики та сфери застосування водяних знаків.Також в роботі представлені найважливіші параметри, для оцінки ефективності ЦВЗ. На основі аналізу сучасного стану методів вбудови ЦВЗ визначили стійкість, непомітність, безпеку та корисне навантаження - основними факторами більшості наукових робіт. Крім того, дослідники використовують різні методи для вдосконалення / збалансування цих параметрів для створення ефективної системи водяних знаків. Наше дослідження визначило основні фактори та нові методики, що використовуються в сучасних дослідженнях. Було запропоновано оцінку ефективності методів вбудови ЦВЗ.

Ключові слова: цифровий водяний знак; автентифікація; LSB; захист авторських прав; цифрові зображення; стеганографія; кібербезпека.

Методология оценки эффективности методов встраивания цифровой водяной знак

И. В. Рубан, Н. Н. Бологова, В. А. Мартовицкий, Р. О. Ярошевич

Аннотация. В последние годы мы наблюдаем значительное увеличение трафика, который проходит через различные сети и каналы. Развитие технологий и глобальной сети приводит к увеличению объема мультимедийного трафика. Для аутентификации и избежания злоупотреблений данные должны быть защищены водяными знаками. В данной работе рассмотрены различные надежные и незаметны методы водяных знаков в пространственной области и области преобразований. Подробно рассмотрены основные понятия цифровых водяных знаков, важные характеристики и сферы применения водяных знаков. Также в работе представлены важнейшие параметры для оценки эффективности ЦВЗ. На основе анализа современного состояния методов встраивания ЦВЗ определили устойчивость, незаметность, безопасность и полезная нагрузка - основными факторами большинстве научных работ. Кроме того, исследователи используют разные методы для совершенствования / сбалансирования этих параметров для создания эффективной системы водяных знаков. Наше исследование определило основные факторы и новые методики, используемые в современных исследованиях. Было предложено оценку эффективности методов встраивания ЦВЗ.

Ключевые слова: цифровой водяной знак; аутентификация; LSB; защита авторских прав; цифровое изображение; стеганография; кибербезопасность.