***Active attacks and natural impacts can lead to two types of image-container distortions: noise-like and geometric. There are also image processing operations, e.g. scaling, rotation, truncation, pixel permutation which are much more detrimental to digital watermarks (DWM). While ensuring resistance to removal and geometric attacks is a more or less resolved problem, the provision of resistance to local image changes and partial image deletion is still poorly understood. The methods discussed in this paper are aimed at ensuring resistance to attacks resulting in partial image loss or local changes in the image. This study's objective is to develop methods for generating a distortion-resistant digital watermark using the chaos theory. This will improve the resistance of methods of embedding the digital watermark to a particular class of attacks which in turn will allow developers of DWM embedding methods to focus on ensuring the method resistance to other types of attacks. An experimental study of proposed methods was conducted. Histograms of DWMs have shown that the proposed methods provide for the generation of DWM of a random obscure form. However, the method based on a combination of Arnold's cat maps and Henon maps has noticeable peaks unlike the method based on shuffling the pixels and their bits only with Arnold's cat maps. This suggests that the method based only on Arnold's cat maps is more chaotic. This is also evidenced by the value of the coefficient of correlation between adjacent pixels close to zero (0.0109) for color DWMs and 0.030 for black and white images***

***Keywords: digital watermarks, chaotic maps, Henon maps, Arnold's cat maps***

UDC 004.93
DOI: 10.15587/1729-4061.2021.246641

# DEVELOPMENT OF METHODS FOR GENERATION OF DIGITAL WATERMARKS RESISTANT TO DISTORTION

**Vitalii Martovytskyi**
*Corresponding author*
PhD, Associate Professor*
E-mail: vitalii.martovytskyi@nure.ua
**Igor Ruban**
Doctor of Technical Sciences, First Vice-Rector**
**Nataliia Bolohova**
Assistant*
**Oleksandr Sievierinov**
PhD, Associate Professor
Department of Information Technology Security**
**Oleg Zhurylo**
Software Developer
Corel Corporation
Landsberger str., 302, Munich, Germany, 80687
**Oleksandr Permiakov**
Doctor of Technical Sciences, Professor
Department of Communication and Automated Control Systems
National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049
**Andrii Nosyk**
PhD, Senior Research
Department of Information Technology and Multimedia Systems
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
**Dmytro Nepokrytov**
Associate Professor
Department of Radioelectronic Systems of Control Points of Air Forces
Ivan Kozhedub Kharkiv National Air Force University
Klochkivska str., 228, Kharkiv, Ukraine, 61045
**Ivan Krylenko**
PhD, Head of Department
Department of Social and Humanitarian Desciplines
Military Institute of Armored Forces of
National Technical University "Kharkiv Polytechnic Institute"
Poltavskyi Shliakh str., 192, Kharkiv, Ukraina, 61000
*Department of Electronic Computers**
**Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

*Received date 21.10.2021*
*Accepted date 02.12.2021*
*Published date 29.12.2021*

***How to Cite**: Martovytskyi, V., Ruban, I., Bolohova, N., Sievierinov, O., Zhurylo, O., Permiakov, O., Nosyk, A., Nepokrytov, D., Krylenko, I. (2021). Development of methods for generation of digital watermarks resistant to distortion. Eastern-European Journal of Enterprise Technologies, 6 (8 (114)), 103–116. doi: https://doi.org/10.15587/1729-4061.2021.246641*

## 1. Introduction

The problem of copyright protection not only remains relevant today but also becomes even more relevant as a continuous process of growth of digital information volumes takes place which requires authorship confirmation. Methods of embedding hidden information in digital multi- and hyperspectral images as well as in video sequences and other digital content

have become widespread in the last two decades in solving the problems of protection against unauthorized copying by means of built-in digital watermarks (DWM) [1]. Digital watermarks have a wide range of applications from copyright protection in the multimedia industry to military secret communications.

The ratio of DWM use in different types of digital content is presented in Fig. 1 and considered in more detail in [2].

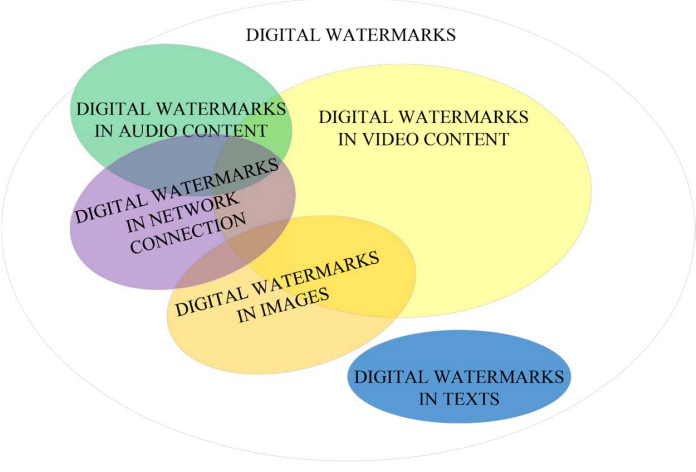



Fig. 1. Venn diagram of basic media capable of supporting digital watermarks

Attacks on steganocontainers are becoming more non-standard with the development of DWM implementation methods. Active attacks and natural distortions can lead to two types of image-container modification: noise-like modifications (changes in pixel values) and geometric modifications (spatial changes in location of pixels).

There are also image processing operations much more detrimental for watermarks, such as scaling, rotation, truncation, pixel permutation. The situation is further complicated by the fact that the DWM can be transformed not only by the violators but also by legal users or be the result of transmission errors in communication channels.

While resistance to removing and geometric attacks is a more or less solved problem, ensuring resistance to local image changes and partial image deletion is still poorly studied.

Therefore, studies aimed at developing the methods and approaches to improve the stability of digital watermarks and do not introduce significant distortions in the image container are relevant. The methods discussed in this paper are aimed at ensuring resistance to attacks resulting in partial image loss or local image changes.

## 2. Literature review and problem statement

A new method of generating 2-D watermarks with good synchronization and secrecy is described in [3]. First of all, the development of a watermark layout resistant to attacks aimed at object cropping and segmentation is presented in [3]. It differs from other existing layouts by its innovative algorithm of template generation. A method of creating a redundant two-dimensional template with cyclic properties depending on the secret key is proposed. However, the disadvantage of this method consists in that it is not resistant to partial image alteration. Also, the scheme of DWM application presented in the study is noticeable to perception by the human visual system.

Study [4] offers an effective method of creating digital watermarks based on biometric data that are unique and can be used in ownership identification. This paper considers the issue of watermark ownership. A biometric sample of fingerprint was used to create a digital watermark. The created watermark was studied for uniqueness and identification ability and used for digital watermarks. The disadvantage consists in that obtaining the digital marks of this type requires special equipment preventing its mass use.

To confirm ownership, it was proposed in [5] to use an effective method of creating digital watermarks based on biometric data, namely iris image. This digital watermark can unambiguously confirm ownership of a digital file. The created watermark was studied for uniqueness and identification ability and used as an audio watermark. When a file is transmitted or the DWM is deliberately attacked, a part of the image with reference points for identification may be lost. In this case, the DWM will be unable to confirm ownership as the number of remaining reference points may not be sufficient to identify the person.

A method of embedding information in video sequences with improved resistance to transcoding is presented in [6]. This method of embedding and removal of textual digital watermarks is based on Arnold's cat barcoding and conversion. It makes it possible to reliably embed and extract textual information from video sequences that can be compressed by high-performance encoding methods when transmitting via insecure communication channels. This method is used to protect copyrights of multimedia product owners.

Existing methods of creating digital watermarks use images with specific patterns or sign images as digital watermarks. Besides, most of these digital data were computed using meaningless pseudo-noise sequences or chaotic functions and were used as digital watermarks. However, these methods do not provide the required stability. Also, such methods have restrictions on the size of the watermark to be inserted into image containers of appropriate size. A method of QR-code creation offered in [7] would be able to use large information volumes as digital watermarks.

To ensure the reliability and security of digital image watermarks, a new algorithm using synergistic neural networks was proposed in [8]. The algorithm first processes a significant image of a gray watermark and then embeds it as a signal in the component of a block discrete cosine transformation (DCT). The accompanying algorithm of watermark detection and extraction uses a cooperative neural network where a suspicious watermark signal is used as an input. The recognition process result is obtained at the output of this algorithm. Modeling experiments show that this algorithm can complete certain image processing operations with improved performance not only by simultaneous completion of detection and removal of watermarks but also by effectively determining the watermark attribution. However, this algorithm can be compromised by competitive attacks on the neural network.

An approach to the creation of watermarks using a logistic map is presented in [9]. Chaotic sequences that can be used to create digital watermarks with the omission of upper or lower frequencies can be generated using this function in combination with the function of initial number generation. One of the disadvantages of using a logistic map consists in the problem of choosing initial parameters of the number generation function when generating chaotic watermarks.

There are many problems with the implementation of methods to ensure copyright protection in images representing open steganosystems. The main ones include the significant partial or complete destruction of digital watermarks when local distortions are introduced into the image container. The methods of DWM generation based on biometric data are not quite effective because of the specifics of obtaining the biometric indicators and sensitivity to any distortion of these data. The use of QR-codes is quite a promising line of development of DWM creation methods but their information redundancy may be their disadvantage.

## 3. The aim and objectives of the study

The study objective is to develop methods for generating distortion-resistant digital watermarks using the chaos theory. This will make it possible to improve the resistance of the DWM embedding methods to a certain class of attacks which in turn will allow developers of embedding methods to focus on ensuring the method resistance to other types of attacks.

To achieve this objective, the following tasks were set:

– analyze of chaotic maps on their ability to ensure the DWM stability;

– develop principles of use of chaotic maps in methods of DWM generation;

– conduct experimental studies on the proposed methods.

## 4. The study materials and methods

Chaotic maps are ascribed to discrete and continuous time domains. Discrete maps usually take the form of repetitive functions that correspond to rounds in cryptosystems. This similarity between cryptography and discrete chaotic dynamic systems is used to develop chaotic cryptosystems. Each map has some parameters equivalent to encryption keys in cryptography. A chaotic system is used in stream ciphers to generate a pseudo-random key stream and a public or secret key is used in block ciphers as initial and control parameter and then the encrypted text is obtained applying a certain number of iterations to chaotic systems. Security and complexity are major issues in cryptosystems. This should be taken into account when choosing a map and its parameters for use in cryptography.

Some chaos-based algorithms provide a good combination of high speed and security at low computing costs. In addition, some chaos-based algorithms and other dynamic systems have many important properties, such as sensitivity to initial parameters, pseudo-random properties, ergodicity, and non-periodicity of generated characters.

Several types of chaotic maps were considered in the study: Arnold's cat maps, Henon maps, logistic chaos maps with key shuffling. This makes it possible to assess their capabilities to ensure DWM sustainability.

In mathematics, Arnold's cat map is a chaotic reflection of a torus in itself named after Vladimir Arnold who demonstrated his studies in the 1960s using images of a cat, hence the map name.

Arnold's cat map is given by the following transformation [11]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}, \quad (1)$$

where $x_{n+1}$ and $y_{n+1}$ are calculated by modulus 1. The mapping of Arnold's cat map is non-Hamiltonian, non-analytical, and shuffling. However, it retains the area because the determinant is equal to 1. Characteristic Lyapunov's indicators are given by the expression:

$$\begin{vmatrix} 1-\sigma & 1 \\ 1 & 2-\sigma \end{vmatrix} = \sigma^2 - 3\sigma + 1 = 0,$$

hence,

$$\sigma_{\pm} = \frac{1}{2}\left(3 \pm \sqrt{5}\right). \quad (2)$$

Eigenvectors are found by substituting $\sigma_{\pm}$ into the matrix equation:

$$\begin{bmatrix} 1-\sigma_{\pm} & 1 \\ 1 & 2-\sigma_{\pm} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \quad (3)$$

The solution for $\sigma_+$ is as follows

$$y = \frac{1}{2}\left(1+\sqrt{5}\right)x \equiv \phi x, \quad (4)$$

where φ is the golden ratio, so the normalized eigenvector is as follows:

$$\xi_+ = \frac{1}{10}\sqrt{50-10\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1}{2}\left(1+\sqrt{5}\right) \end{bmatrix}. \quad (5)$$

Similarly, the solution for the σ is as follows

$$y = -\frac{1}{2}\left(1-\sqrt{5}\right)x \equiv -\phi^{-1}x, \quad (6)$$

and the normalized eigenvector is:

$$\xi_- = \frac{1}{10}\sqrt{50+10\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1}{2}\left(1-\sqrt{5}\right) \end{bmatrix}. \quad (7)$$

That is, with a measurement unit equal to the width of a square image, the image is cut one unit up, then two units to the right. Everything outside this unit square is shifted one unit back until it is inside the square.

The Henon map, sometimes called the Enon-Pomo attractor/map [12], is a dynamic system with discrete time. This is one of the most studied examples of dynamic systems that demonstrate chaotic behavior. Henon map takes a point $(x_n, y_n)$ in the plane and maps it to a new point by the formula [13]:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n. \end{cases} \quad (8)$$

The map depends on two parameters, $a$ and $b$ which have values $a$=1.4 and $b$=0.3 for the classical Henon mapping. For classical signs, Henon mapping is chaotic. For other values of $a$ and $b$, the map may be chaotic, intermittent, or converge to a periodic orbit.

A logistic map is a one-dimensional discrete chaotic map that can generate chaotic behavior using a simple nonlinear

dynamic equation. Mathematically, the logistic map is determined by the following equation [14]:

$$x_{n+1} = rx_n(1-x_n), \quad (9)$$

where $r$ (sometimes denoted by μ) is a positive constant known as the "biotic potential" giving the so-called logistic map. This square map can behave in a very complicated manner. This is the nonlinear equation designed to describe two effects:

– reproduction where the population will grow at a rate proportional to the current population when the population size is small;

– starvation (density-dependent mortality) at which the growth rate will decrease at a rate proportional to the value obtained by adopting the theoretical "bearing capacity" of the environment minus the current population.

## 5. The results obtained in studying the methods of generating distortion-resistant digital watermarks

### 5. 1. Analysis of chaotic maps on their ability to ensure the digital watermark stability

The chaos theory is used in many scientific disciplines: mathematics, biology, computer science, economics, engineering, finance, philosophy, physics, politics, psychology, and robotics. It affirms that complex systems are highly dependent on initial conditions and small changes in the environment can lead to unpredictable consequences.

The chaos theory has been used in cryptography for many years. Over the past 10 years, chaos theory and nonlinear dynamics have been used in the development of hundreds of cryptographic primitives. These algorithms include image encryption algorithms, hash functions, secure generators of pseudo-random numbers, stream ciphers [15].

To analyze the suitability of using the chaotic maps to create stable digital marks, three variants of chaotic maps were chosen: logistic map, Henon maps, and Arnold's cat maps.

Analysis of image histograms and autocorrelation between adjacent pixels were used to analyze the results of initial image transformation by logistic maps.

Image histogram analysis is one of the simplest methods to demonstrate the encryption quality. A good method of encrypting images tends to turn plain text images into a random, incomprehensible form. Thus, a good image encryption technique makes it possible to generate an encrypted image with evenly distributed histogram intensity.

Because images have a high information redundancy, it is desirable to have an encryption algorithm that violates this redundancy. Thus, the correlation between adjacent pixels in horizontal, vertical, or diagonal directions is found as an indicator of encryption efficiency. The horizontal direction was considered here. 1024 random pixels were selected from the image, then the correlation of pixels with the extreme right neighbor was determined. For a good algorithm, the correlation graph can be random, without any noticeable pattern.

As presented in Fig. 2, the initial image that was used in the study had the size of 200×200. Fig. 3, 4 present a histogram of the initial image from Fig. 2 for each channel: R, G, and B, respectively, and its autocorrelation with adjacent pixels.

The image histogram shows a certain relative number of pixels with a certain brightness at a given color depth of the image. It was assumed that the abscissa (i. e. horizontal axis) is for the image brightness values (either total or for one of the channels, e. g. as in the RGB model with three such channels: R, G, and B, respectively). The ordinate (i. e. vertical axis) is for the relative numbers (or even percentage) of pixels of a certain brightness.


Fig. 2. Initial image

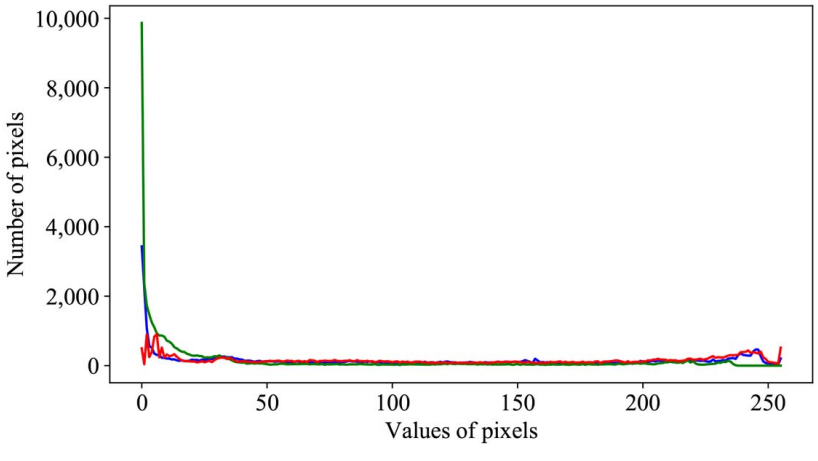



Fig. 3. Histogram of initial image

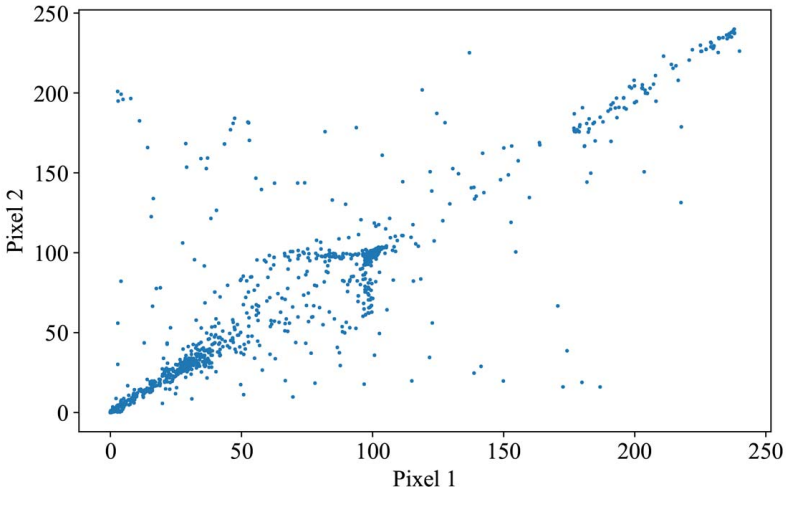



Fig. 4. Correlation of pixels in initial image and with their extreme right neighbors

Fig. 3 shows the usual distribution of pixel brightness for each channel separately and the correlation of pixel values with their right neighbors is shown in Fig. 4.

The image was first encrypted with Arnold's cat maps with the following algorithm steps.

*Step 1.* Set parameters for the algorithm work $k$, where $k$ is the number of pixel shuffling iterations.

*Step 2.* Shuffle all pixels of the image according to (1) and repeat this iteration $k$ times.

Thus, the encrypted image was obtained which is presented in Fig. 5. Fig. 6, 7 show the histogram of encrypted image and autocorrelation between adjacent pixels.

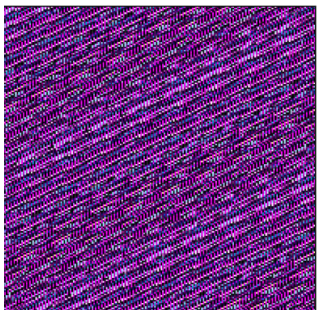


Fig. 5. The image was encrypted using Arnold's cat maps; $k$=44

Fig. 6 shows that Arnold's cat maps in no way violate the pixel brightness distribution (Fig. 3 and Fig. 6 are the same). However, the application of Arnold's cat maps shows a more chaotic distribution of pixels compared to the initial image as evidenced by the chorogram image presented in Fig. 7.

The following image encryption algorithm has been proposed to use Henon maps. Using (8), a sequence of bits of length 200×200×8 was generated: if $x_n$<=0.4, then the corresponding bit is 1. Next, the sequence was transformed into a two-dimensional array of 200×200 with each element bitwise summed with the initial image. Fig. 8 shows the image after shuffling the pixel bits and Fig. 9, 10 show the encrypted image histogram and autocorrelation between adjacent pixels.

Fig. 9 shows that because of bitwise summing, the Henon map violates pixel brightness distribution since the distribution of pixel brightness is chaotic over the entire range of brightness values for each of the channels. A more chaotic distribution of pixels can also be seen compared to the initial image. It is evidenced by the correlogram image presented in Fig. 10.

The algorithm based on logistic maps works similarly to the algorithm of Henon maps with one exception: values for each pixel are sequentially recalculated according to (9) and bitwise summed up. Encrypted images are formed in this way.

Fig. 11 shows an image after shuffling the pixel bits using a logistic map. Fig. 12, 13 show a histogram of the encrypted image and autocorrelation between adjacent pixels.

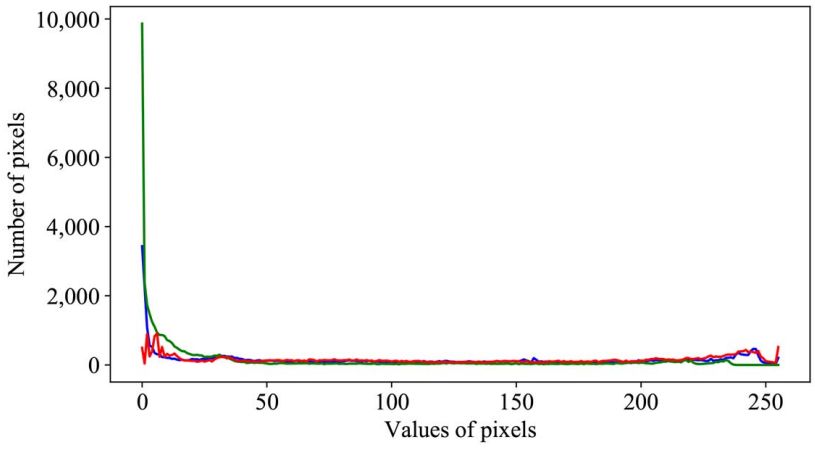



Fig. 6. Histogram of the image after shuffling with the help of Arnold's cat maps

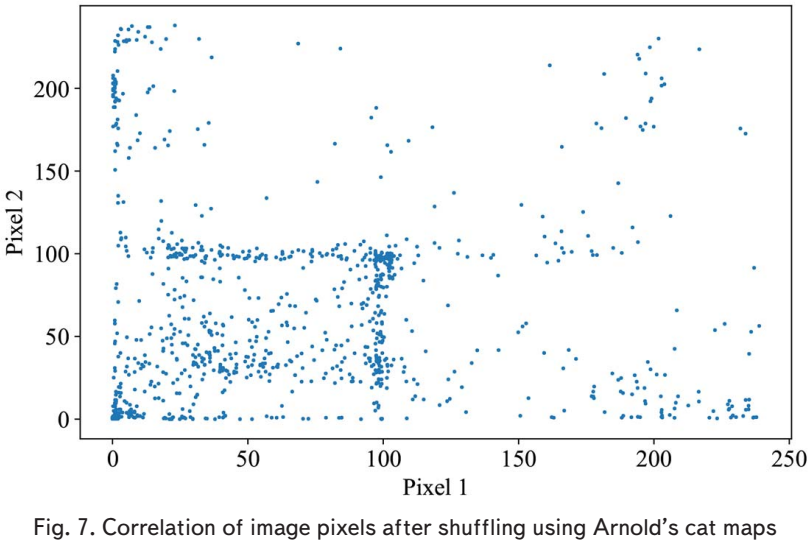



Fig. 7. Correlation of image pixels after shuffling using Arnold's cat maps

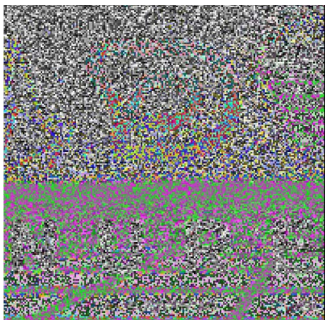


Fig. 8. The image was encrypted using Henon maps; initial values: ($x_0$, $y_0$)=(1.1, 1.3)

As can be seen from Fig. 12, 13, brightness values of the image pixels have a chaotic nature of distribution and do not correlate with each other.

Thus, when analyzing the results of using chaotic maps of various types, the following conclusions can be drawn:

– due to spatial changes in pixel location, Arnold's cat maps provide resistance to local distortion. However, because of the fact that these maps in no way violate distribution of pixel brightness, the invisibility of such DWM incorporation in the container will suffer;

– on the contrary, due to the chaotic distribution of pixel brightness, Henon and logistic maps will ensure the invisibility of such a DWM after its embedding since the DWM in the container will look like an additive noise.

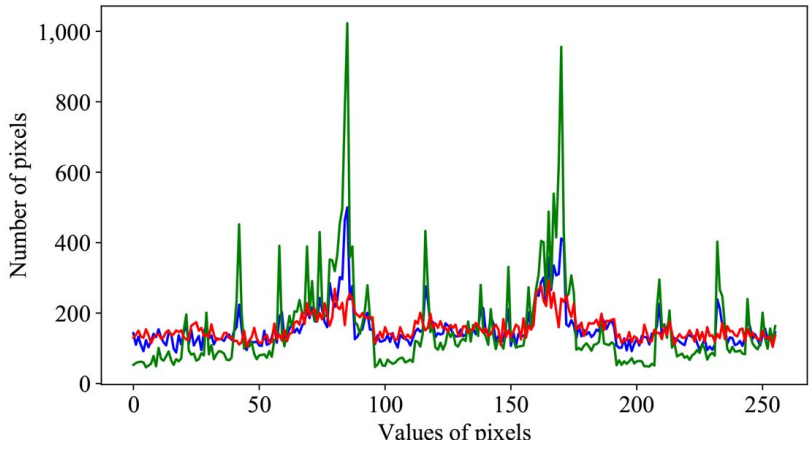



Fig. 9. Histogram of the image after shuffling the pixel bits using Henon maps

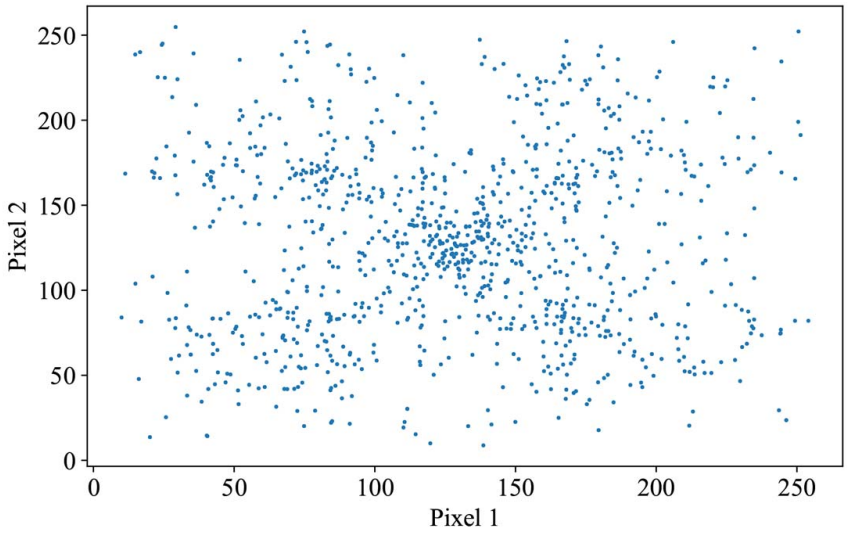



Fig. 10. Correlation of image pixels after shuffling pixel bits using Henon maps

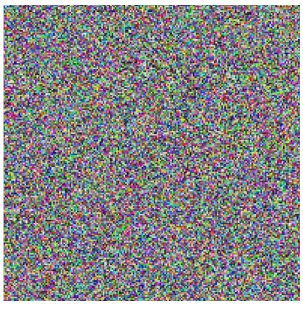


Fig. 11. The image was encrypted with the help of logistic maps

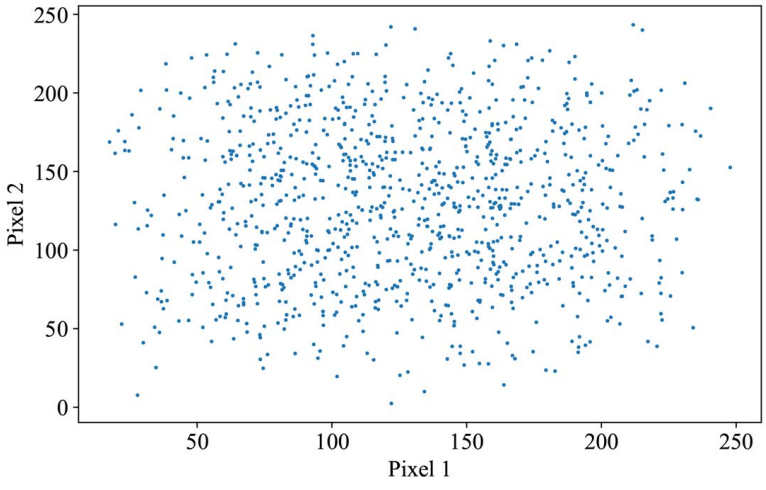



Fig. 12. Histogram of the image after shuffling the pixel bits with the help of logistics maps

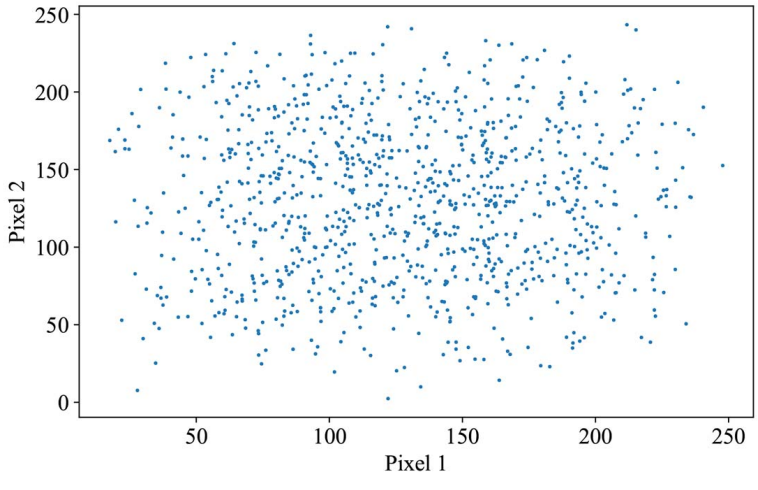



Fig. 13. Correlation of the image pixels after shuffling the pixel bits using logistics maps

**5. 2. The principles of using chaotic maps in the methods of digital watermark generation**

Proceeding from the above analysis of the current state of studies and taking into account current trends in the field of information security, it was proposed to use tokenization technology to identify users.

Tokenization is the process of turning confidential data into insensitive data, so-called "tokens" that can be used in a database or internal system without entering them into sight. Tokenization can be used to protect sensitive data by replacing initial data with unrelated values of the same length and format. The tokens are then sent to the organization's internal systems for use and the initial data are stored in a secure token repository. Unlike encrypted data, tokenized data cannot be decrypted and are irreversible. This difference is especially important because there is no mathematical relationship between the token and its source number and tokens cannot be turned back to their initial form [16].

To achieve the invisibility of applying the DWMs on digital content, it is desirable to use the DWMs that are identical in their nature to the embedded object [7, 11]. Thus, it is proposed to convert tokens of the copyright holders into one of the varieties of the QR code. This is necessary to present the token in an image form, thus ensuring the invisibility of the DWM in the image.

Two methods of DWM generation are presented. Their principles are similar. They differ in the complexity of private keys and computational complexity although they use the same general principle.

The method of generation of a stable DWM consists of two units: a unit of DWM generation and encryption and a unit of DWM decryption and additional filtering. The method includes the following steps:

*Step 1*. Initialization of the method parameters. *P, Q* are parameters for shuffling images using Arnold's cat maps, *k* is the number of pixel shuffling iterations, (*x, y*) are parameters for generating an array of bit masks using Henon maps. Initialization of a unique token image and size of the DWM itself.

*Step 2*. Generation of QR code based on the token and its placement in the DWM image.

*Step 3*. Shuffling the DWM *k* times using expression (10).

*Step 4*. A sequence of bits of length $m \times m \times 8$ is generated using (8) where *m* is the DWM size in pixels. If $x_n <= 0.4$, then the corresponding bit is 1. Next, the sequence is converted into a two-dimensional array of size $m \times m$.

*Step 5*. Each element of the array of bit masks obtained in Step 4 is bitwise added to the mixed DWM obtained in Step 3. As a result, the DWM is obtained.

The decryption process includes the following steps:

*Step 1*. Initialization of the method parameters. *P, Q* are parameters for shuffling images using Arnold's cat maps; *k* is

the number of pixel shuffling iterations; ($x$, $y$) are parameters for the generation of an array of bit masks using Henon maps. Initialization of the DWM.

*Step 2*. Shuffling the DWM $k$ times using expression (11).

*Step 3*. A sequence of bits of length $m \times m \times 8$ is generated using (8) where $m$ is the DWM size in pixels. If $x_n <= 0.4$, then the corresponding bit is 1. Next, the sequence is converted into a two-dimensional array of size $m \times m$.

*Step 4*. Each element of the bit mask array obtained in Step 3 is bitwise added to the mixed DWM obtained in Step 2.

*Step 5*. QR codes applied on the DWM are removed.

*Step 6*. The QR codes obtained in the previous step are bitwise summed and the obtained QR code is filtered.

*Step 7*. The QR code is scanned and the image token is obtained.

The unit of generation and encryption is presented in Fig. 14.

This method is based on Henon and Arnold's cat maps. The image token, DWM size, initial coordinates ($x$, $y$) to generate an array of bit masks and parameters for image shuffling (the number of shuffling iterations $k$), and parameters $P$, $Q$ (10) are fed to the method input.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(m). \quad (10)$$

The process of DWM generation involves the generation of a token-based QR code and applying it on the DWM image which must be larger than the QR code size. This procedure is necessary to provide additional resistance to a certain type of attack on the DWM and will be used at the additional filtering stage. For example, a token-based QR code has a size of 40×40 pixels and the requirement to the DWM size indicates that it should be 200×200 pixels. Thus, 4 copies of the QR code are applied on the DWM to provide additional resistance to distortion. Besides, this can be used to further filter the DWM after image decryption and increase the likelihood of error-free decryption of the image token.

The filtration process consists of two stages:

*Stage 1*. Shuffling the image pixels $k$ times (10) to ensure the resistance of the entire DWM to local changes.

*Stage 2*. Shuffling the bits of each pixel separately to ensure DWM security.

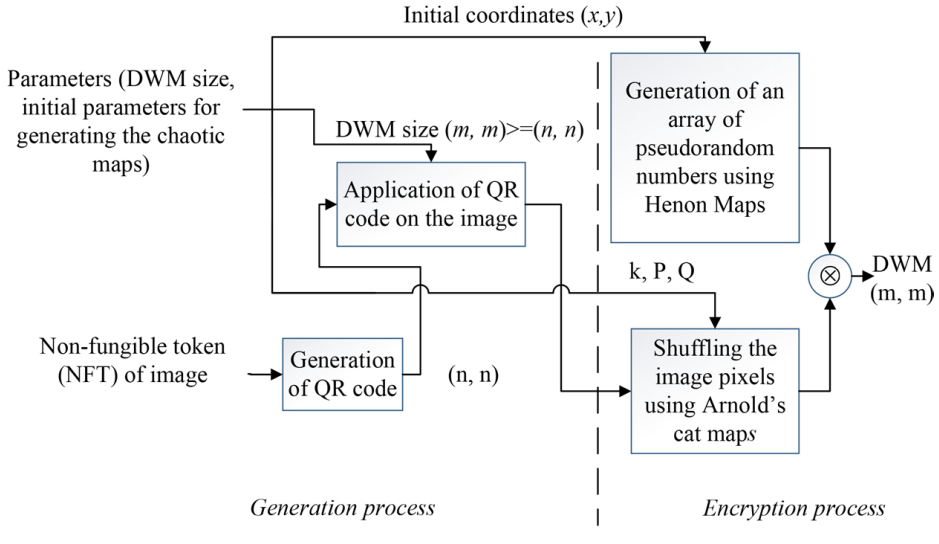



Fig. 14. Block diagram of the generation and encryption unit

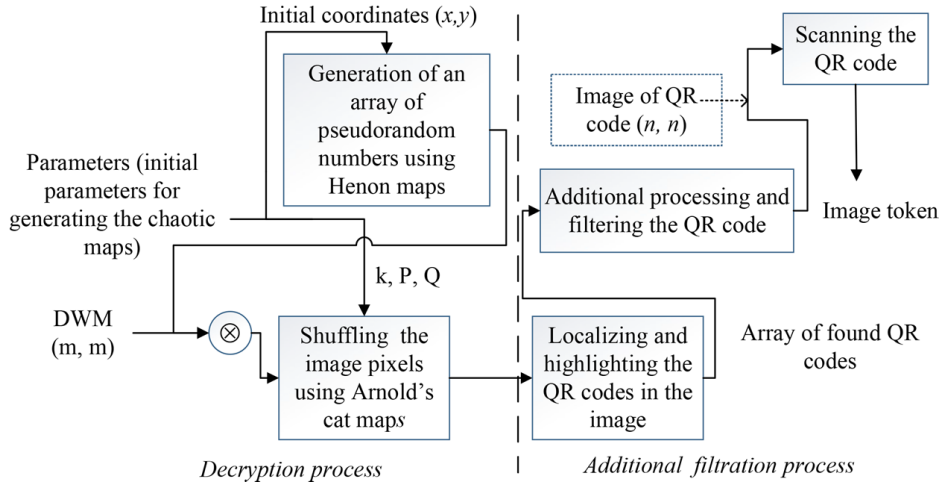



Fig. 15. Block diagram of the unit of decryption and additional filtering

The unit of DWM decryption and additional filtering is presented in Fig. 15.

The DWM image and parameters for generating Henon maps (10) and back-shuffling the image using Arnold's cat maps (the number of shuffling iterations $k$ and parameters $P$, $Q$ (11)) are fed to the input to decrypt and obtain the token. The reverse operation of shuffling the image pixels is performed with the help of these parameters.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} PQ+1 & -P \\ -Q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(m). \quad (11)$$

The decryption process involves the use of a bit mask for each pixel of the image and then, the reverse shuffling operation is performed $k$ times according to (11).

The additional filtering process includes the localization of all instances of QR codes. Then, if more than one QR code is found, each pixel can be added bit by bit and the resulting image filtered.

It was proposed to use cell averaging and subsequent binarization as a filtration method. As evidenced by the results presented in [17], this filter was chosen on the basis of previous studies.

The binarization threshold $\tau$ is found by the Otsu algorithm or using adaptive binarization [18].

The second method of DWM generation is similar in principle to the first one but the process of shuffling the pixels and bits of an individual pixel occurs simultaneously on the basis of Arnold's cat maps and includes the following steps:

*Step 1*. Initialization of the method parameters. $P$, $Q$ are parameters for shuffling the image using Arnold's cat maps; $k$ is the number of iterations of pixel shuffling. Initialization of a unique image token and size of the DWM itself.

*Step 2*. Generation of QR code based on the token and its application on the DWM image.

*Step 3*. Shuffling the DWM pixels $k$ times using the expression (10) and shuffling the pixel bits using the algorithm shown in Fig. 18. As a result, the required DWM is obtained.

The decryption process includes the following steps:

*Step 1*. Initialization of the method parameters. $P$, $Q$, are parameters for shuffling the image using Arnold's cat maps; $k$ is the number of iterations of pixel shuffling. Initialization of the DWM.

*Step 2*. Shuffling the DWM $k$ times using expression (11) and shuffling the pixel bits using the algorithm shown in Fig.18 in which formula (11) is used instead of (10).

*Step 3*. Removal of QR codes inserted in the DWM.

*Step 4*. Bitwise summing up the QR codes obtained in the previous step and filtering the resulting QR code.

*Step 5*. Scanning of the QR code and obtaining the image token.

Fig. 16, 17 present the process of generation and decryption of DWM, and Fig. 18 presents the algorithm of the shuffling process.

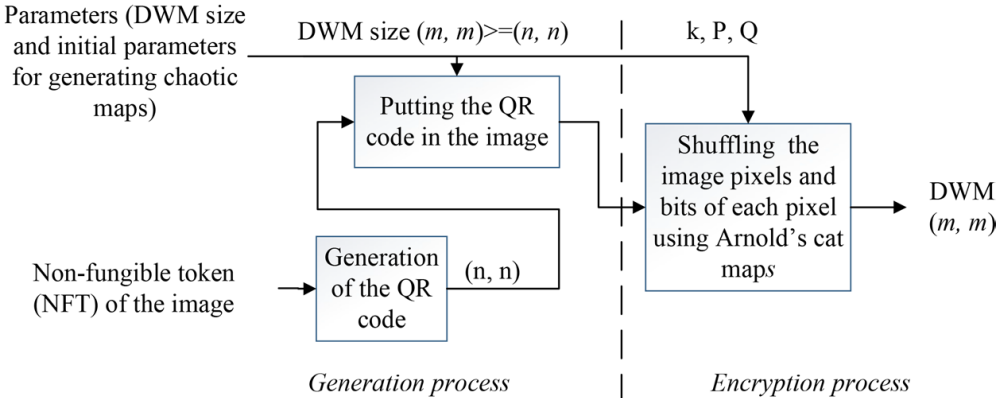



Fig. 16. Generation of a digital watermark based on Arnold's cat maps

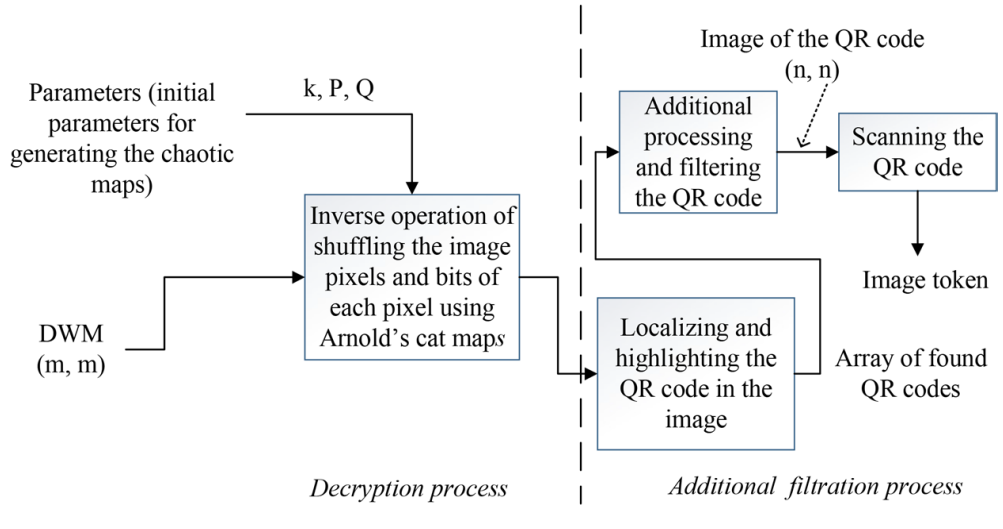



Fig. 17. Description of a digital watermark based on Arnold's cat maps

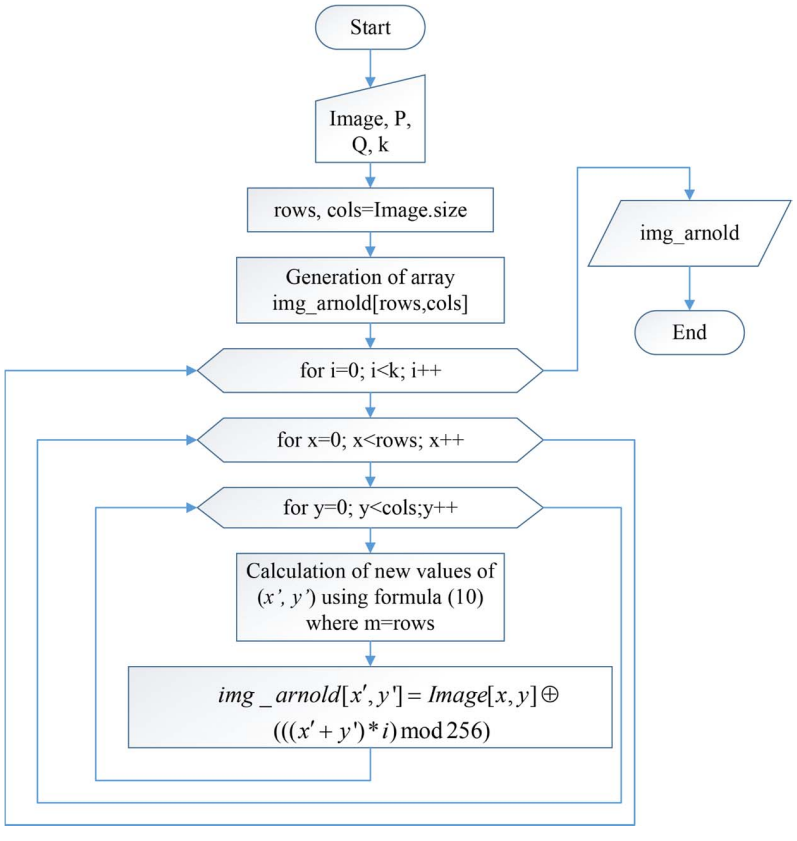



Fig. 18. Algorithm of shuffling the image pixels and pixel bits

The back-shuffling algorithm works similarly to the algorithm presented in Fig. 18 but (11) is used instead of (10) and renewal of bits of each pixel is calculated using the formula:

$$\text{img\_arnold}[x',y'] = \\ = \text{Image}[x,y] \oplus \left((x+y)*(k-i) \bmod 256\right). \quad (12)$$

This method of DWM generation is of less computational complexity and has a high level of security at relatively simple key values.

### 5. 3. Experimental study of digital watermark generation methods

To conduct the experiments, a token was generated for the image shown in Fig. 2. The token structure is presented in Fig. 19.

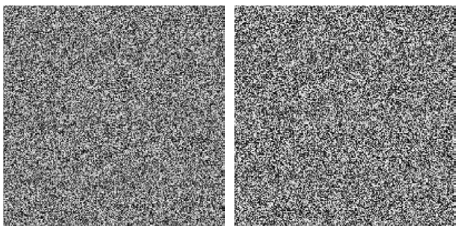
Based on this token, a QR code with dimensions of 159×159 was generated which according to the proposed method was placed in the center of the DWM having a size of 200×200. This DWM is presented in Fig. 20.

The next step of the algorithm consists in shuffling the DWM. Fig. 21, *a* shows shuffling using Arnold's cat maps and Henon maps (Fig. 14) and Fig. 21, *b* shows shuffling using only Arnold's cat maps (Fig. 1, *b*).

```
{
"timeStamp": 1635776636
"autorID" : "6f70f283-d004-41f6-b0a0-3fe6b4110f63"
"imageHash" : "9a5a2825297c096890c063f0fdc7d3b0"
"prevBlock" : "507257de2915a9186f4275fc1ff86eefd5b2543636bc5db409da4562f90e89a2"
}
```

Fig. 19. Structure of the Image token

Fig. 20. The generated QR code of the token placed in the digital watermark



*a* *b*

Fig. 21. The digital watermark after shuffling: *a* – using Arnold's cat maps and Henon maps (*x, y*)=(1.1,1.3); *b* – *P*=2, *Q*=1; *k*=5 (; using Arnold's cat maps and Henon maps *P*=2; *Q*=1, *k*=5

To study the security of the generation methods, histograms of the DWM images were constructed, Fig. 22; DWM after shuffling, Fig. 23, 24.

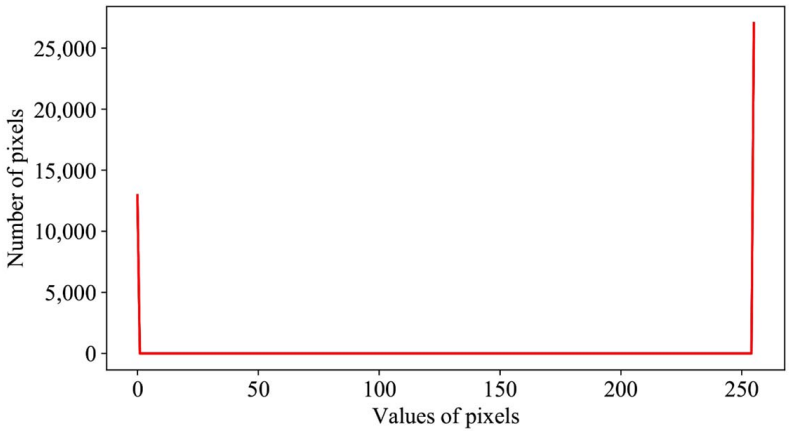



Fig. 22. Histogram of a digital watermark shown in Fig. 20

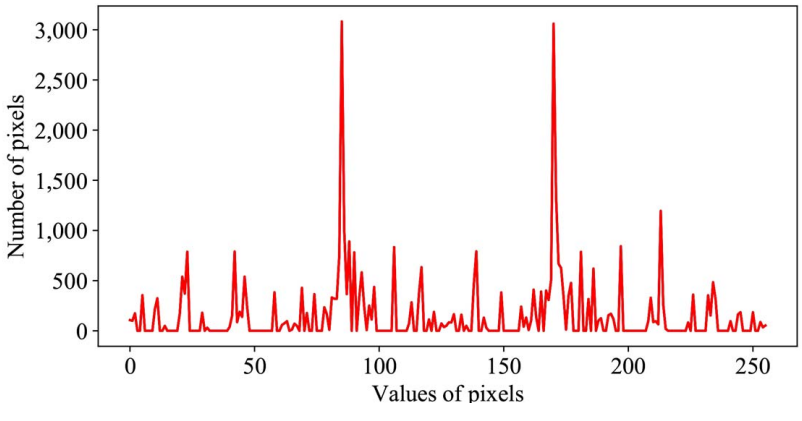



Fig. 23. Histogram of a digital watermark after shuffling with the help of Arnold's cat maps and Henon maps (Fig. 21, *a*)

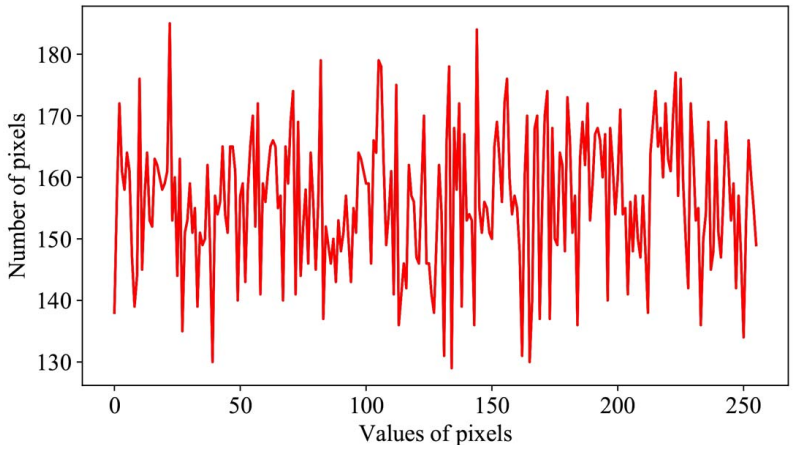



Fig. 24. Histogram of a digital watermark after shuffling with the help of Arnold cat maps (Fig. 21, *b*)

Correlation between adjacent pixels in the horizontal direction was found as an indicator of encryption efficiency. 1024 random pixels were selected from the image and correlation with the far-right neighbor was determined and displayed. The diagram of the correlation of the DWM from Fig. 20 is shown in Fig. 25. Correlation after shuffling is shown in Fig. 26, 27.

To demonstrate the stability of the DWM forming method, a graph of the percentage of deleted pixels vs. the percentage of incorrectly restored pixels of the initial DWM was constructed (Fig. 28).

Table 1 shows values of correlation coefficients for a color image and for a binary image (the QR code).

Table 1

Values of the correlation coefficient for neighboring pixels

| Type of transformation | Color image from Fig. 2 | Binary image from Fig. 20 |
|---|---|---|
| Original | 0.877 | 0.73 |
| Arnold's cat maps | 0.034 | 0.052 |
| Henon maps | 0.027 | 0.038 |
| Logistic maps | 0.005 | 0.034 |
| Arnold's cat maps+ +Henon maps | 0.011 | 0.028 |
| Arnold's cat maps | 0.0109 | 0.030 |

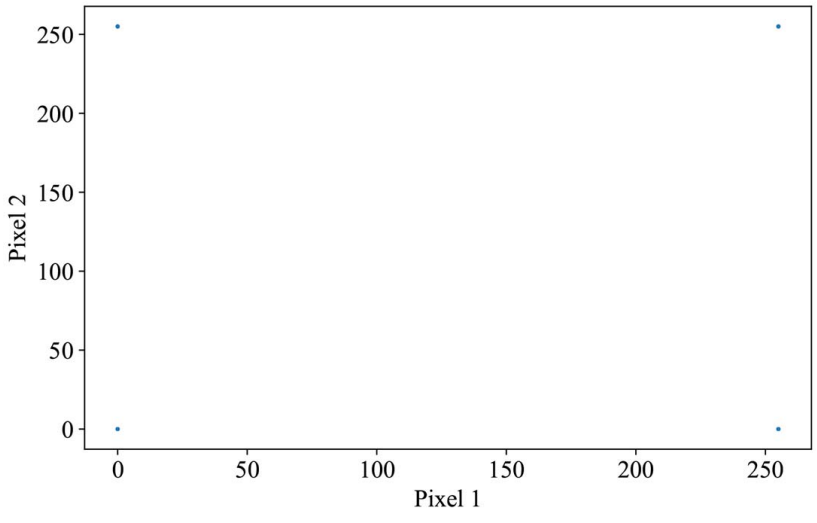



Fig. 25. Correlation of pixels of a digital watermark shown in Fig. 20

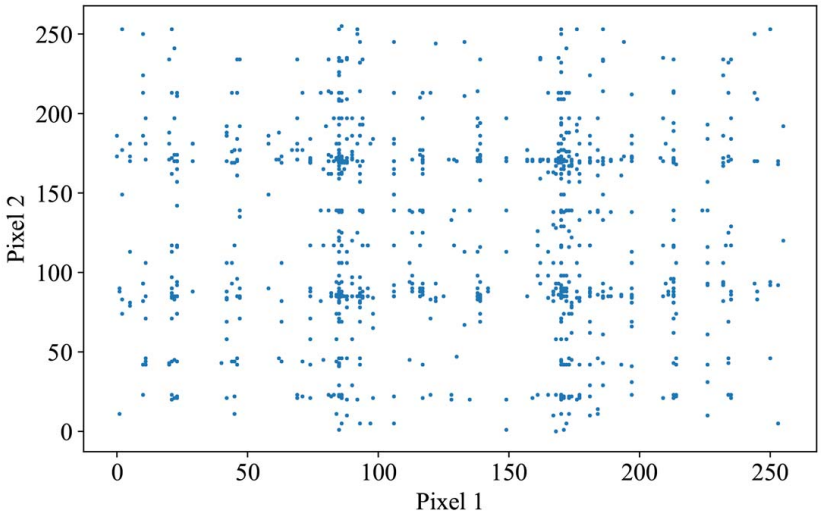



Fig. 26. Correlation of pixels in a digital watermark after shuffling using Arnold's cat maps and Henon maps from Fig. 21, *a*

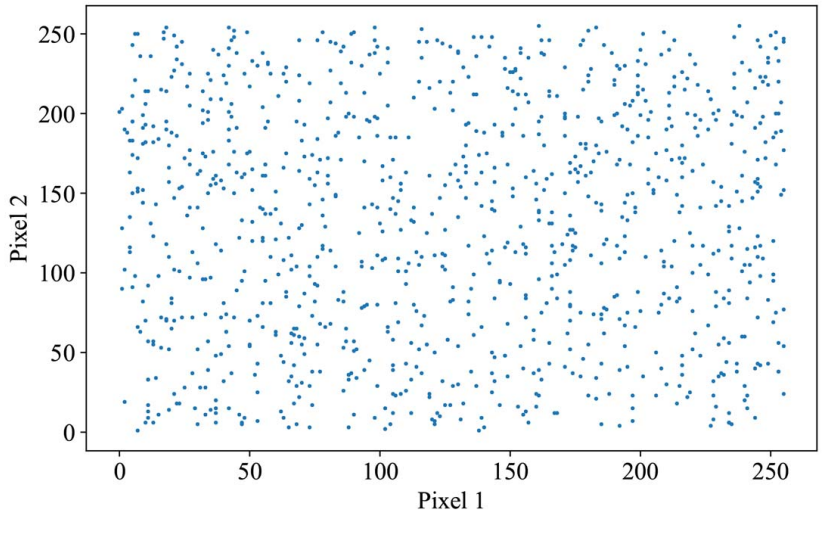



Fig. 27. Correlation of pixels in a digital watermark after shuffling using Arnold's cat maps from Fig. 21, *b*

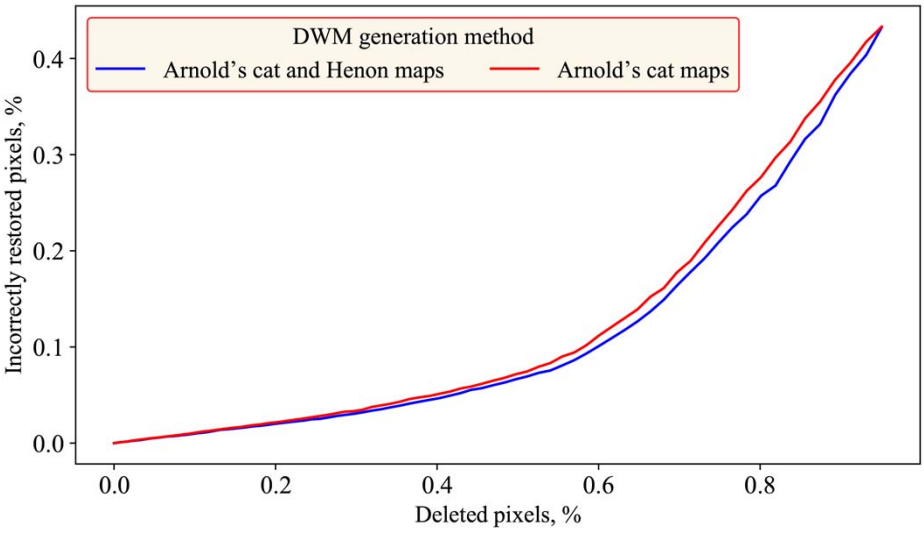



Fig. 28. Plot of the ratio of lost pixels to correctly restored pixels

Fig. 28 shows that both methods of DWM generation provide correct recovery of almost 90 % of pixels at 60 % lost pixels

## 6. Discussion of the results of studying the methods of generating the distortion-resistant digital watermark

To analyze the results of studying the methods, the DWM histograms were considered (Fig. 22–24). It can be seen from the histograms (Fig. 26, 27) that both methods enable the generation of DWMs of a random, obscure form. However, the method based on a combination of Arnold's cat maps and Guenon's maps (Fig. 14, 15) has noticeable peaks in contrast to the method based on shuffling pixels and their bits with Arnold's cat maps alone. This is evidence of obtaining more chaotic DWM using the method presented in Fig. 16–18.

It can be concluded from Table 1 that both methods provide an acceptable level of protection because the coefficient of correlation between adjacent pixels is relatively small. Hence, it is almost impossible to statistically detect such a DWM after installation not to mention its decryption without exact values of the key.

When considering the graph shown in Fig. 28, it can be affirmed that both methods are quite resistant to local pixel distortion since almost 90 % of the QR code can be recovered at a 60 % destruction of the DWM.

In contrast to the methods of DWM generation presented in [4, 5], a token is used as an identifier of the property right. The Proof-of-Work consensus algorithm can be applied when generating the token. Unlike biometric data, it does not require any additional equipment and protects distributed systems against abuse. A QR code is used in [7] as a DWM, however, the presented methods are devoid of disadvantages of common QR codes due to shuffling and additional filtering. This is discussed in detail in [19].

Shuffling of image pixels has been proposed to ensure DWM stability since the randomness of pixel arrangement secures resistance to local changes in the DWM itself. It can be concluded from analysis of the results obtained (Fig. 21–28), that the proposed methods of DWM generation are capable of improving the stability of DWM embedding methods.

The limitation of the proposed methods consists in the fact that the size of the QR code generated based on the image token should be less than or equal to the DWM size. This, in turn, will lead either to the inability to use the presented methods with this procedure of tokenization or to revising the requirements to the DWM itself.

The disadvantage of the proposed methods includes the fact that one of the mechanisms of ensuring resistance to distortion is achieved consists in information redundancy. Therefore, to further develop the proposed methods and technologies of copyright protection, it is planned to conduct studies using codes capable to correct errors.

## 7. Conclusions

1. Chaotic maps were analyzed in order to ensure DWM stability. Analysis has shown that the use of chaotic maps to shuffle bits of pixels or the pixels themselves in the image can provide security and resistance to distortion. Calculations of the coefficient of correlation of neighboring pixels when using chaotic maps indicate the efficiency of their use. Because images have a high information redundancy, it is desirable to have an algorithm that will remove this redundancy.

2. Methods of DWM generation based on chaotic maps and additional filtering of digital watermarks have been developed. The methods described in this paper are effective for ensuring the DWM resistance to local distortions. Studies have shown that it is possible to restore 90 % DWM with a 60 % image distortion.

3. Experimental study of the proposed methods was conducted. Histograms of the DWM have shown that both methods provide generation of SWMs of a random, obscure form. However, the method based on a combination of Arnold's cat maps and Henon maps has noticeable peaks in contrast to the method based on shuffling pixels and their bits with Arnold's cat maps alone. This indicated that the method based only on Arnold's cat maps produces more chaotic DWMs. This is also evidenced by the value of the coefficient of correlation between adjacent pixels which is close to zero: equal to 0.0109 for color DWMs and 0.030 for black and white images.

References

1. Mitekin, V. A. (2015). An algorithm for generating digital watermarks robust against brute-force attacks. Computer Optics, 39 (5), 808–817. doi: https://doi.org/10.18287/0134-2452-2015-39-5-808-817

2. Artru, R., Roux, L., Ebrahimi, T. (2019). Digital watermarking of video streams: review of the state-of-the-art. arXiv.org. Available at: https://arxiv.org/pdf/1908.02039.pdf
3. Delannay, D., Macq, B. (2000). Generalized 2-D cyclic patterns for secret watermark generation. Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101). doi: https://doi.org/10.1109/icip.2000.899230
4. Dutta, M. K., Singh, A., Soni, K. M., Burget, R., Riha, K. (2013). Watermark generation from fingerprint features for digital right management control. 2013 36th International Conference on Telecommunications and Signal Processing (TSP). doi: https://doi.org/10.1109/tsp.2013.6614031
5. Dutta, M. K., Singh, A., Burget, R., Atassi, H., Choudhary, A., Soni, K. M. (2013). Generation of biometric based unique digital watermark from iris image. 2013 36th International Conference on Telecommunications and Signal Processing (TSP). doi: https://doi.org/10.1109/tsp.2013.6614024
6. Zotin, A., Favorskaya, M. (2020). Application of bar coding for digital watermarking of video sequences based on frequency transforms. Information and Control Systems, 5, 12–23. doi: https://doi.org/10.31799/1684-8853-2020-5-12-23
7. Cho, D.-J. (2013). Study on Method of New Digital Watermark Generation Using QR-Code. 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications. doi: https://doi.org/10.1109/bwcca.2013.102
8. Li, D., Deng, L., Bhooshan Gupta, B., Wang, H., Choi, C. (2019). A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Information Sciences, 479, 432–447. doi: https://doi.org/10.1016/j.ins.2018.02.060
9. Mooney, A., Keating, J. G., Heffernan, D. M. (2006). A detailed study of the generation of optically detectable watermarks using the logistic map. Chaos, Solitons & Fractals, 30 (5), 1088–1097. doi: https://doi.org/10.1016/j.chaos.2005.09.029
10. Schöpf, H.-G. (1970). V. I. Arnold and A. Avez, Ergodic Problems of Classical Mechanics. (The Mathematical Physics Monograph Series) IX + 286 S. m. Fig. New York/Amsterdam 1968. W. A. Benjamin, Inc. Preis geb. $ 14.75, brosch. $ 6.95 . ZAMM - Zeitschrift Für Angewandte Mathematik Und Mechanik, 50 (7-9), 506–506. doi: https://doi.org/10.1002/zamm.19700500721
11. Peterson, G. (1997). Arnold's cat map. Available at: http://anyflip.com/jwch/llux
12. Hsu, C. S. (1987). Cell-to-cell mapping: a method of global analysis for nonlinear systems. Springer, 354. doi: https://doi.org/10.1007/978-1-4757-3892-6
13. Wu, J., Liao, X., Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. Signal Processing, 153, 11–23. doi: https://doi.org/10.1016/j.sigpro.2018.06.008
14. Ye, G., Huang, X. (2017). An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing, 251, 45–53. doi: https://doi.org/10.1016/j.neucom.2017.04.016
15. Akhavan, A., Samsudin, A., Akhshani, A. (2011). A symmetric image encryption scheme based on combination of nonlinear chaotic maps. Journal of the Franklin Institute, 348 (8), 1797–1813. doi: https://doi.org/10.1016/j.jfranklin.2011.05.001
16. What is Tokenization? Available at: https://www.tokenex.com/resource-center/what-is-tokenization
17. Makoveichuk, O., Ruban, I., Bolohova, N., Kovalenko, A., Martovytskyi, V., Filimonchuk, T. (2021). Development of a method for improving stability method of applying digital watermarks to digital images. Eastern-European Journal of Enterprise Technologies, 3 (2 (111)), 45–56. doi: https://doi.org/10.15587/1729-4061.2021.235802
18. Bradley, D., Roth, G. (2007). Adaptive Thresholding using the Integral Image. Journal of Graphics Tools, 12 (2), 13–21. doi: https://doi.org/10.1080/2151237x.2007.10129236
19. Makoveychuk, O. (2019). A new type of augmented reality markers. Advanced Information Systems, 3 (3), 43–48. doi: https://doi.org/10.20998/2522-9052.2019.3.06