Encryption of Dynamic Areas of Images in Video based on Certain Geometric and Color Shapes

NASHAT AL BDOUR
Computer and Communication Engineering,
Tafila Technical University,
Tafila,
JORDAN

Abstract: - The paper is devoted to the search for new approaches to encrypting selected objects in an image. Videos were analyzed, which were divided into frames, and in each video frame, the necessary objects were detected for further encryption. Images of objects with a designated geometric shape and color characteristics of pixels were considered. To select objects, a method was used based on the calculation of average values, the analysis of which made it possible to determine the convergence with the established image. Dividing the selected field into subregions with different shapes solves the problem of finding objects of the same type with different scales. In addition, the paper considers the detection of moving objects. The detection of moving objects is carried out based on determining the frame difference in pixel codes in the form of a rectangular shape. Cellular automata technology was used for encryption. The best results were shown by the transition rules of elementary cellular automata, such as: 90, 105, 150, and XOR function. The use of cellular automata technologies made it possible to use one key sequence to encrypt objects on all video frames of the video. Encryption results are different for the same objects located in different places of the same video frame and different video frames of the video sequence. The video frame image is divided into bit layers, the number of which is determined by the length of the code of each pixel. Each bit layer is encrypted with the same evolution, which is formed by one initial key bit sequence. For each video frame, a different part of the evolution is used, as well as for each detected object in the image. This approach gives different results for any objects that have a different location both on the video frame image and in different video frames. The described methods allow you to automate the process of detecting objects on video and encrypting them.

Key-Words: - encryption, image, cellular automata, key array, image section, object image detection, evolution, Wolfram's rule.

Received: May 15, 2022. Revised: January 23, 2023. Accepted: February 19, 2023. Published: March 29, 2023.

1 Introduction

In modern society, information technology has reached such a stage of development that video is used in almost all areas of human activity. Video surveillance systems of various structures and various functional purposes are widely used. Now information about various events in most cases is presented using video. However, there are cases when the video contains various prohibited content that occupies insignificant areas in the field of the video display. Such content can be images: cigarettes, alcohol, naked body, prohibited signs, and others. The presence of prohibited images imposes a ban on all videos. In this case, the video can be shown, and prohibited areas can be hidden (filled with one color, for example, white). Such areas are usually defined by the user and hidden by the user. Existing approaches are based on the formation of another video with hidden image areas. This is necessary to save the original image, which results in the use of additional memory. There are also areas of the image on the video that carry confidential or secret information. Such areas of the image must be encrypted. At the same time, the encryption-based approach does not require additional memory, since it can be determined using the encryption and decryption key and does not require the formation of additional video.

One of the main functions for hiding parts of the video image is the function of searching and selecting the specified images that may appear in some video frames during the entire video. Searching for such areas in the image by the user leads to a lot of time.

To automate the process and increase the reliability of the selection of specified areas, it is necessary to use methods for automatically detecting such areas in each video frame for further encryption.

The objective of the research is to increase the reliability of the selected areas and reduce the time spent on processing all video frames based on methods that use process automation. Also, the task is to detect dynamically changing objects in the video (moving, resizing, etc.), which are fixed using rectangular selection windows. Selected forms on each video frame are encrypted using cellular automata (CA) technologies, which allows solving the problem of using the optimal size encryption key when encrypting large amounts of video data.

All modern works aimed at creating methods for detecting and selecting a graphic object by geometric and color structure are divided into two large groups, [1], [2]: generalizing and distinguishing. Generalizing methods are based on building a given model of the image of the detected object and assessing the accuracy of the model of the new image found in the visual picture based on this model. The most popular generalizing methods are, [2], [3]: random field model, [4], [5], implicit form model, [6], constellation model, [7]. The main characteristics of the methods using these models are presented in [2].

The second group of methods based on the difference is that a known classifier is created or used, with the help of which the differences between the negative and positive images of a particular training sample are determined. The best-known difference-based methods are the Viola-Johnson, [8], LeCun, [9], and Papageorgiou, [10], methods. Comparative characteristics of these methods are presented in the table in [2].

Both groups of methods and each of the methods in each specific case of solving a specific problem are the most effective. Influencing factors are: performance, memory size, implementation complexity, and other parameters. Systems that implement methods for selecting objects in the visual picture use the training mode and the mode of direct search and selection of an object.

In [11], the selection of objects is based on the perception and action in a three-dimensional scene from different points of view. The results obtained in this work allow you to select objects in a complex visual environment.

Among the works devoted to image encryption in this paper, attention is paid to partial image encryption on each video frame of the video. In general, all existing methods, [12], [13], [14], [15], [16], [17], [18], that are aimed at image encryption can be used to encrypt parts of images. The analysis of works devoted to image encryption was carried out in [19], [20], [21]. The works, [22], [23], describe methods for encrypting parts of an image. These methods use selective encryption of the specified image area based on unique attributes, such as image frequency, total brightness, special compression area, etc., [23], [24], [25], [26], [27], [28].

The most promising methods for partial image encryption are methods using cellular automata technologies, [19], [21], [29], [30]. This technology makes it possible to reduce the key length, as well as to reduce the time it takes to encrypt image sections in all frames of the analyzed video.

2 Method for Searching for Homogeneous Objects on Video Frames

The simplest method is to enumerate the numerical values of the codes of each pixel in the image of each video frame for subsequent comparison of the sequence of numbers with the reference sequence that must be selected on the image of each frame. However, this method is time-consuming. In this method, small differences in codes can lead to false results that make it impossible to select the desired area.

To select an area on an image, this paper uses the method of calculating the average value for the entire selected area and for its individual sections, [31]. In this case, the average values of all selected areas must be strictly ordered. The average value is calculated for all values of the pixel codes belonging to the image area of a given size, and the allowable interval is set, within which the image area is determined by the given average value. Such a method is described in detail in the paper, [31], for selecting the human auricle in the image.

It is necessary to take into account the size of the image area to be selected. The size of the image area can be set in advance by the user. In this case, a false selection of an image area of a given size is possible. An example of such a false selection is shown in Figure 1.

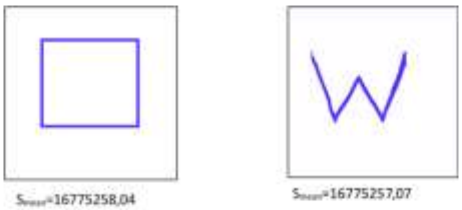

Fig. 1: An example of a false selection of an image area of a given size based on the average value.

Figure 1 shows that the images are different, but they have the same average values (the difference is 0.97018888). In this case, the image structure of the selected area is not determined. Only one quantitative value is determined, which does not carry information about the structure of the image and the distribution of color and brightness characteristics in it.

The structure of the image and the distribution of color and brightness characteristics are determined by dividing the selected area into smaller areas, and the necessary selection of such areas is also carried out. Options for splitting the images are shown in Figure 1 and on a smaller area in Figure 2.

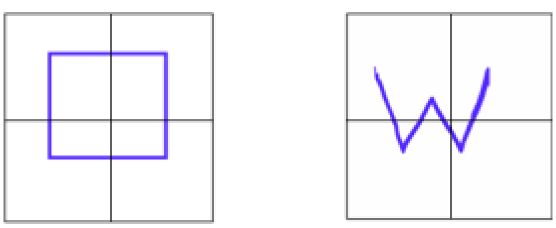

Fig. 2: Options for partitioning the images shown in Fig. 1, on a smaller area.

In Figure 2, the partitioning options are shown with a different number of subareas and with different locations. As can be seen from Figure 2, different geometric shapes fall into each field, which accordingly leads to different average values. For the left image (Figure 2), the average values can be represented as a matrix

$$I_{left} = \begin{bmatrix} 16775031{,}06 & 16775045{,}5 \\ 16775472{,}75 & 16775484{,}3 \end{bmatrix},$$

and for the right image (Figure 2) the matrix of averages has the following values

$$I_{right} = \begin{bmatrix} 16775020{,}18 & 16775455{,}47 \\ 16774979{,}47 & 16775553{,}76 \end{bmatrix}.$$

Accordingly, the difference between such average values for each selected area shows that the images are different. The matrix of difference values has the following form

$$I_{\text{difference}} = \begin{bmatrix} 10{,}87577 & -409{,}9482 \\ 493{,}2837 & -69{,}47198 \end{bmatrix}.$$

In this case, four rectangular regions are used, so the arrays of averages can be represented as two-dimensional arrays, which simplifies the processing of the obtained data.

In the case of using video in each video frame, image fragments may be distorted. This is due to the video filming, the distance to the video camera, etc. Changing the distance to the video camera entails a change in the scale of both the entire image and individual sections of the images of each video frame.

In such situations, controlled areas of video with the same picture elements and different scales cannot be determined using average values. Therefore, to identify images in each video frame, a matrix of ratios of the average values of all sub-areas into which the controlled area of images is divided is used

$$R = \begin{vmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{vmatrix}$$

The relationship matrix R has a size of n×m (where n is the number of sub-areas along the X-coordinate and m is the number of sub-areas along the Y-coordinate). The more sub-areas, the higher the accuracy of image identification. However, the processing speed is reduced, which is unacceptable for processing video sequences in real-time. In addition, to process the quantitative values of the relationship matrix R, it is necessary to use special algorithms and form a base of reference matrices R_{ref}. However, the construction of such a matrix is possible for rectangular areas in the image.

If it is necessary to select images of certain geometric shapes with specified color and brightness characteristics, then the formation of different shapes of subareas and their number is carried out. Figure 3 shows different options for the shape of sub-regions for different images.

Fig. 3: Variants of the forms of sub-areas into which controlled areas of images are divided for different images

Figure 3 shows that different shapes and different numbers of sub-areas can be used for different images (separated by light lines in each image). For each option, a sequence vector of quantitative values obtained from the analysis of each subarea is formed. In general, the vector structure has the form

$$R_f = \langle r_{f_1}, r_{f_2}, \dots, r_{f_k} \rangle,$$

where r_{f_i} - average value for i - th subarea.

In this case, for each variant, a rigid arrangement of the sequence of numbers in the vector is set. To sequentially compare the numbers inside the vector with the reference ones, the first ones should be the average values of those sub-areas that carry the greatest amount of information about the entire selected area. If there are scale changes on the image, then a matrix of numbers is formed that corresponds to the relationship between all average values of the vector of average values. In this case, subareas are also formed taking into account large-scale changes in the entire selected area of the video frame image. In accordance with scale changes and different shapes of images of the selected areas of the image, the relationship vectors also have different sizes.

Based on the considered approaches, an important task is to find the optimal shapes and location of subdomains that provide the most information in the analysis of the selected area.

3 Detection of Moving Objects in the Visual Scene

In many areas, some tasks are aimed at detecting and hiding moving objects on the video scene. To solve such problems, the video is divided into a sequence of video frames, each of which is an image, and if there is movement in the video, then the images of the video frames are different. At the same time, pictures can change completely in adjacent video frames on the video. In this case, a large number of pixels are allocated that have changed their codes in two adjacent video frames. In practice, the entire image in each subsequent video frame can be selected. Among such changes in the entire background of the image, it is very difficult to distinguish a moving object.

This work is aimed at detecting not only moving objects on a weakly changing video background but also detecting moving objects that have certain geometric shapes. If the background of the entire image does not change, but only the analyzed object changes (its location changes), then the solution to this problem is simplified. If the general background in adjacent video frames of the video changes, then the solution to the object selection problem becomes more complicated, since there is an additional task of preliminary identification of the moving area of the video frame image. And in this case, the preliminary capture of the moving image area is not always used.

To select a moving object without significant changes in the background, this work uses an algorithm for calculating the difference in the codes of two pixels of adjacent video frames located on the same coordinates. This method is described in detail in [32], [33]. The method is quite simple and is widely used in solving various problems of image processing. A pixel-by-pixel comparison of codes in two adjacent video frames is carried out. Pixels are determined that, compared to pixels in previous frames, have changed their color and brightness code. Selected pixels capture motion on the analyzed video. All other pixels are defined as pixels belonging to the background of the image.

The selection of the moving area is carried out by selecting a rectangular area, which is determined by the selected pixels (Figure 4).

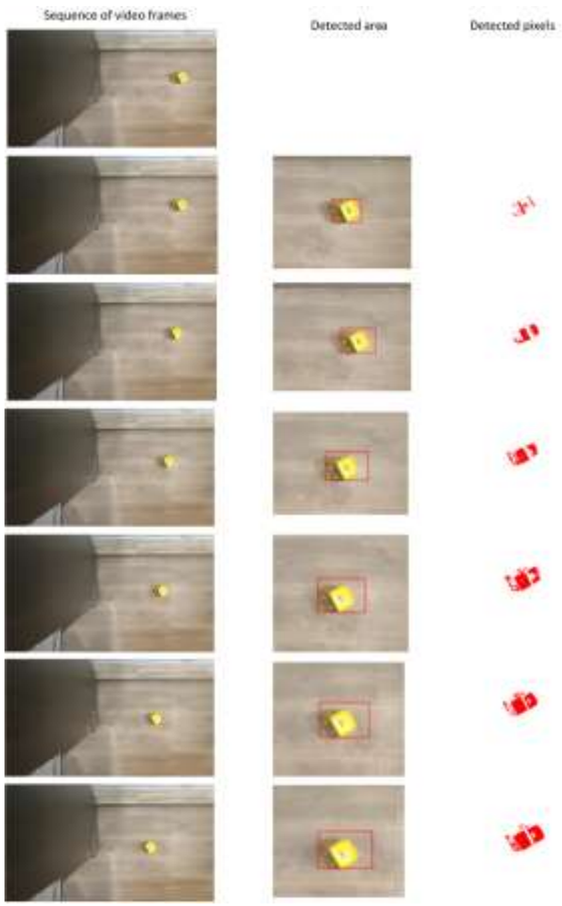

Fig. 4: An example of selecting an area of a selected object using the algorithm for determining the difference in pixel codes in adjacent video frames

Figure 4 shows a rectangular area describing the moving object. The yellow robot movement sequence starts from the top (initial video frame). The right side of the highlighted area indicates where the robot was in the previous video frame. This example shows that the size of the selected area can change. It all depends on other transformations of the selected area (rotation, scaling, etc.). A different number of pixels are selected for each frame.

Also, to detect moving objects, the algorithm for superimposing several adjacent frames of the video stream can be used. In this case, the difference in pixel codes is calculated or a bitwise XOR operation is performed for all pixels. All matched bits and codes become black, and non-matched bits form codes of other colors that form the selected pixels.

Another thing is when the background of the whole picture in neighboring video frames changes completely and more than 90% of the pixels are highlighted (according to the algorithm discussed above) as participating in motion. In this case, the most appropriate selection algorithm is an algorithm that uses the calculation of average values and the construction of a matrix of relations that allows you to identify the desired area of the image. Using an algorithm based on the calculation of average values allows us to select stationary areas.

In addition, this approach allows the selection of areas with the same geometric shape, but different colors (codes) of pixels (Figure 5).

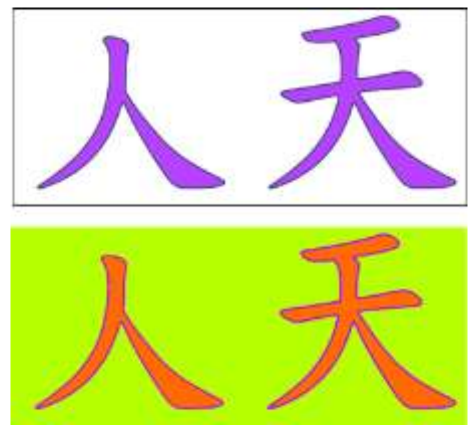

Fig. 5: Examples of images of the same geometric shapes, but with different colors

To solve the problem, the image is preliminarily binarized (Figure 6) and the necessary average values are calculated with division into subareas. In binary images, it is easier to determine the average values and set the shapes of the subareas.

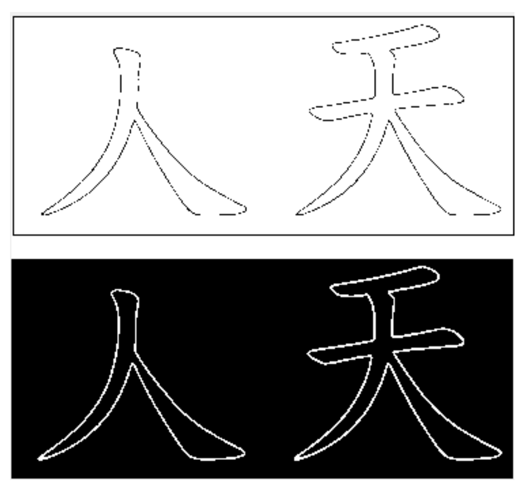

Fig. 6: Examples of binarization of images presented in Fig. 5. The brightness level during binarization is set to 50%

After converting the original image into a bitmap, the subarea shapes are selected, the average values are calculated, and the relationship matrix is formed.

4 Encryption of Selected Areas of the Image

To encrypt selected areas on video, there is a need to encrypt such a section in each video frame. For this, one encryption key can be used for the image of each video frame. However, if the image of the selected area in each video frame has the same geometric and luminance-color structure, then the encryption result will also be represented by the same image. This approach to encrypting video sequences is not always acceptable. For example, several different areas can be selected in one visual picture. Accordingly, the video will display different selected areas with the same encryption results.

To solve the problem of separating encryption areas by encryption keys, as well as by encryption methods, it is necessary to use additional methods for their specific and effective application. Since stream encryption is most often used, it is enough to separate the key pseudo-random bit sequence and use each part of it as a key sequence for each selected image area in each video frame.

One of the options for such encryption is the use of a pseudo-random number generator based on CA with active cells, [29], [30], [31], [32], [33], [34]. Such a method is described in [20]. This paper shows that it is enough to use the three most significant bits in each color byte of the image for encryption. However, although this approach gives high image quality, it is time-consuming and not always acceptable.

To reduce the time spent when encrypting individual sections of the sequence, it is advisable to use the methods described in [19], [20], [21]. In these works, CAs are also used to generate the encryption key. In this case, the original key sequence has a length equal to the dimension of the video frame (vertical or horizontal image). The initial key sequence determines the initial state of the elementary CA (ECA).

Based on the initial states of the ECA and the selected transition rule, a two-dimensional evolution is formed, which coincides in dimension with the image size of the frame of the analyzed video sequence. An example of encryption of selected areas on the image of one video frame in Figure 7 is shown.

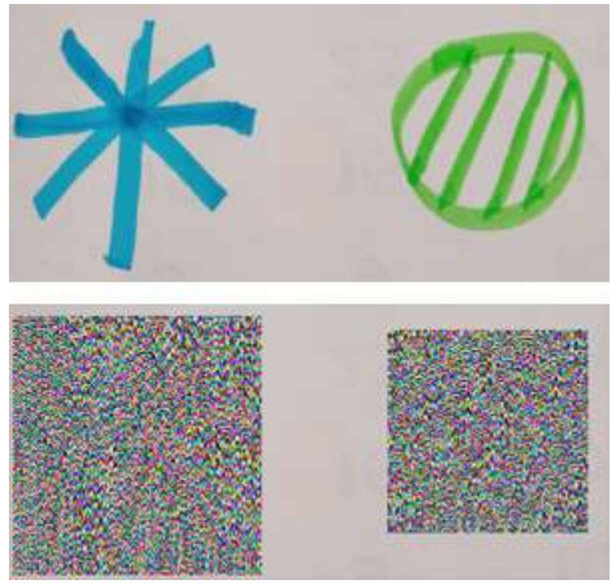

Fig. 7: An example of encryption of selected areas on the image of one video frame using two-dimensional ECA evolution. The transition function of 105 ECA is used with a shift by one step of evolution

Figure 7 shows the original image of a video frame with selected areas (on the left) and the same image with encrypted areas that are selected in the original image. The image shows that the selected areas have different color and brightness structures. In this case, the original image has the same selected areas.

The process of encrypting the selected areas of the image is to perform the following functional steps.

1. The video into sequences of video frames is divided.
2. In the image of each video frame, a given area of the image is selected.
3. The encryption of the selected areas using the selected encryption method is carried out.
4. A new video is formed from a sequence of video frames with encrypted image sections.

The first stage is implemented using a variety of software and hardware video recording and video generation.

The resulting sequence of video frames is analyzed in the second stage in order to select the necessary image areas present in the images of each video frame. Such areas can be rectangular areas that highlight moving objects, as well as areas with a certain geometric and color structure. To select each of these areas, methods that allow you to do this were previously considered.

To encrypt selected areas (third stage), the necessary time costs are taken into account. If the number of video frames is large, then the use of the method of generating a pseudo-random key gamut leads to a large time expenditure. Although the method showed high reliability of encryption. The most acceptable is the method that uses CA to form a key array, [19], [20], [21]. The method shows particular efficiency in cases where there are several different selected areas on the images of video frames. The choice of the encryption method also takes into account the fact that the encrypted areas of the images should differ in color structure for the images of all video frames.

In the fourth stage, a video is formed in which there are encrypted areas.

To encrypt the selected areas of the image, a method is used that forms a key array based on the CA. Rules are used: 90, 105, 150, and XOR functions, [21], examples of which in Figure 8 are shown.

Fig. 8: Examples of key arrays formed based on ECA evolution using rules 90, 105, 150, and XOR functions. The XOR function uses the analysis of six neighboring cells (three at each step of evolution) in the previous two steps of evolution

Sections of key arrays, which coincide in a location with the selected sections on the images of video frames, are the corresponding selected key arrays for each selected area. Since the key arrays differ throughout the field of the created evolution, the encryption result for each selected area is also different. This situation allows us to hide the fact that the same information is hidden in each video frame. Examples of encryption of identical selected areas with different locations on the image of one video frame in Figure 9 are shown, and examples of encryption of different areas using the same key array in Figure 10 are shown.

Fig. 9: An example of encryption of identical selected areas with different locations on the image of one video frame. Rule 105 was used with a shift by one step of evolution

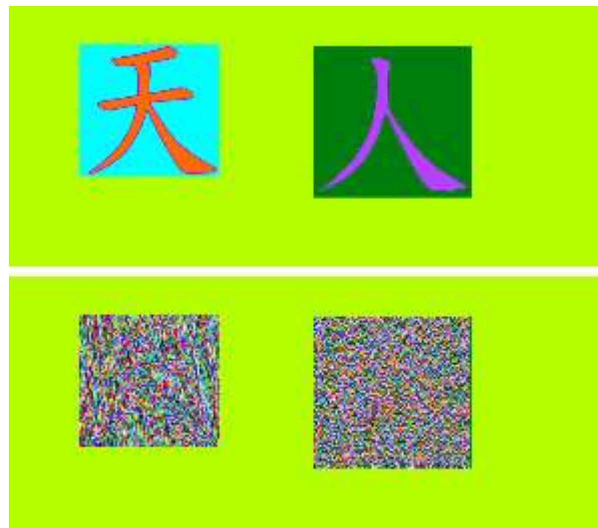

Fig. 10: An example of encryption of different selected areas on the image of one video frame. The XOR function was used, taking into account neighboring cells of the two previous steps of evolution

As can be seen from Figure 9 and Figure 10, the structures of images obtained as a result of encryption are different, which determines the high quality of encryption.

If you use the same key array to encrypt all video frames, then for stationary selected areas, the encryption results in all video frames being the same. If dynamically changing areas or areas that change their location are selected, then the encryption results of such areas differ.

Improving the quality of encryption is achieved by using different key arrays for each video frame. The formation of such arrays can be achieved by various methods. One such method is to use different ECA transition rules that give the best encryption quality. Such rules are studied and described in [21].

The use of different rules allows you to form different key arrays on the same initial states of the ECA. However, a large number of video frames does not allow using a separate ECA transition rule with the same initial settings for each video frame. Therefore, the paper proposes to use an approach based on increasing the number of evolutionary steps, which allows increasing the key array and using its fragments to encrypt the image of each video frame. This approach allows you to use only one key sequence for the entire video. This key sequence is bit-based and forms the initial states of the ECA used to form the corresponding evolution. The key sequence can be represented in either decimal or binary codes. An example of such video encryption on individual video frames in Figure 11 is shown.

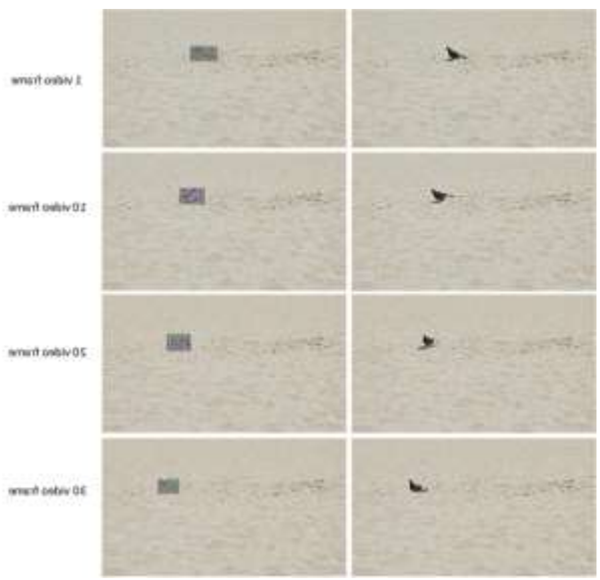

Fig. 11: An example of encryption of selected areas based on one key sequence and different key arrays for each video frame

In Figure 11 are stationary selected areas with different encryption results in each video frame.

An approach was used to form key arrays, which consists of the formation of one initial key sequence. All bit layers into which the image of the video frame was divided were encrypted using the generated key arrays. The key array was formed using the formation of ECA evolution according to a given transition rule. For each bit layer, the key array began with different evolution time steps. In the same way, the formation of key arrays for the bit layers of the image of each video frame was carried out. In fact, only one initial key sequence is chosen, and different "shifted" key arrays are used for encryption, which are taken from the generated evolution. Combinations of different transition rules can also be used.

One key sequence represents ECA early in evolution. As a rule, its length corresponds to the dimension of the image. From one key sequence, many evolutions can be formed, which is determined by the number of ECA transition rules used according to Wolfram. Each image of a video frame is divided into binary layers, the number of which is equal to the length of the code (number of bits) that goes into encoding the color characteristics of each pixel. If three bytes are used to encode one pixel (1 byte is the red code, 1 byte is the green code, and 1 byte is the blue code), then the image is divided into 24 binary layers.

The generated evolution (key two-dimensional array) has a higher dimension than the binary layer. An evolution fragment is used to encrypt each binary layer. As a rule, each fragment of evolution for each subsequent binary layer begins with each subsequent time step of evolution. This will make it possible to use different key arrays to encrypt objects in different video frames.

This approach allows you to get different images after encryption for the same image sections both in one and in different video frames.

5 Conclusion

The paper considers the process of detecting objects on frames of a video sequence to encrypt them. Using a method based on calculating the average values of the selected area and dividing the area into sub-areas allows selecting of objects of a given geometric structure and color range, as well as selecting the same shapes, changed to scale. An experiment was conducted that showed that cellular automata are best suited for selecting and encrypting images of identical objects with different locations. Cellular automata make it possible to form a high-dimensional evolution that gives different key arrays for all selected objects in video frames. The initial key array is a bit sequence indicating the initial state of the elementary cellular automata. The rules that give high-quality encryption (90, 105, 150, and XOR function based on two previous evolution steps) are defined. In this case, only one rule can be used to encrypt all video frames.

In further research, the author plans to use cellular automata that implement the detection of different and identical objects on video. The research will also focus on the use of two-dimensional cellular automata.

References:

[1] Roth, P.M. Survey of Appearance-Based Methods for Object Recognition / P.M. Roth, M. Winter // Technical Report ICG-TR-01/08, Institute for Computer Graphics and Vision, Graz University of Technology, Austria, January, 2008. – p. 68

[2] A.N. Alfimtsev, I.I. Lychkov. The Technique of Real-Time Object Detection in the Video Stream. Вестник ТГТУ. 2011. Том 17. № 1. Transactions TSTU. pp. 44-55.

[3] Murphy, K.P. Models for Generic Visual Object Detection / K.P. Murphy // Technical report, Department of Computer Science, University of British Columbia, Vancouver, Canada, May, 2005. – p. 8

[4] Stan Z. Li, "Markov Random Field Modeling in Image Analysis", Computer Science Workbench, Springer, 2001. p. 323

[5] Gimel'farb G.L., "Image Textures and Gibbs Random Fields", Kluwer Academic Publishers: Dordrecht, 1999. p. 250

[6] Greenspan, M. Efficient Tracking with the Bounded Hough Transform / M. Greenspan, L. Shang, P. Jasiobedzki // Proceedings of Computer Vision and Pattern Recognition. – 2004. – Vol. 1. – p. 520–527.

[7] Fergus, R. Object Class Recognition by Unsupervised Scale-Invariant Learning / R. Fergus, P. Perona, A. Zisserman // Proceedings of Computer Vision and Pattern Recognition. – 2003. – Vol. 2, Sec. II. – p. 264–271.

[8] Viola, P. Robust Real-Time Object Detection / P. Viola, M. Jones // *Intl. J. Computer Vision.* – 2004. – Vol. 57(2). – p. 137–154.

[9] LeCun, Y. Learning Methods for Generic Object Recognition with Invariance to Pose and Lighting / Y. LeCun, F.-J. Huang, L. Bottou // Proceedings of Computer Vision and Pattern Recognition. – 2004. – Vol. 2. – p. 97–104.

[10] Papageorgiou, C.A Trainable System for Object Detection / C. Papageorgiou, T. Poggio // Intl. J. Computer Vision. – 2000. – Vol. 38(1). – p. 15–33.

[11] Mela Francisco. Active Object Detection: An Active Perception Approach to Object Detection. Thesis for: MSC Mechatronics Engineering. Advisor: Serhan Cosar

[12] Stepan Bilan, Andrii Demash. High performance encryption tools of visual information based on cellular automata. - Information Technology and Security. - 2016. - Vol. 4, № 1(6). - С. 62-75.

[13] Xingyuan Wang, Dapeng Luan. (2013). A novel image encryption algorithm using chaos and reversible cellular automata. Communications in Nonlinear Science and Numerical Simulation 18(11):3075–3085

[14] A.L.A. Dalhoum, A. Madain, H. Hiary, Digital image scrambling based on elementary cellular automata, Multimedia Tools Appl. 75 (24) (2016) 17019–17034.

[15] T.H. Chen, M. Zhang, J.H. Wu, C. Yuen, Y. Tong, Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling, Opt. Laser Technol. 84 (2016) 118–133.

[16] Wassim Alexan, Mohamed khaled Elbeltagy. (2021). Lightweight Image Encryption: Cellular Automata and the Lorenz System. Conference: 2021 International Conference on Microelectronics (ICM): 34-39.

[17] Juan Contreras , Marco Ramírez , Jesús Aboytes. Image Encryption System Based on Cellular Automata and S-Box. Research in Computing Science 148(10), 2019. pp. 153–161

[18] Wang Y, Zhao Y, Zhou Q, et al. (2018) Image encryption using partitioned cellular automata. Neurocomputing 275:1318–1332

[19] Nashat Albdour, Image encryption methodology based on cellular automata, Journal of Theoretical and Applied Information Technology, 2022. Vol.100. No 23.

[20] Nashat Albdour and Ayman M Mansour Optimal steganographic protection method based on image encryption, Przegląd Elektrotechniczny, 2021, Vol.97. No 6.

[21] Nashat Albdour,Selection of Intelligent Rules for the Evolution of Elementary Cellular Automata for Image Encryption, WSEAS Transactions on Systems and Control 2022, Vol.17.

[22] Marc Van Droogenbroeck. Partial encryption of images for real-time applications. Fourth IEEE Signal Processing Symposium

[23] Wonyoung Jang. Sun-Young Lee. Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment. International Journal of Distributed Sensor Networks 2020, Vol. 16(3). pp. 1-17.

[24] Kumari S. A research paper on cryptography encryption and compression techniques. Int J Eng Comput Sci 2017, 6(4): 20915–20919.

[25] Kaur M and Kumar V. A comprehensive review on image encryption techniques. Arch Comput Method Eng 2018, 27: 15–43.

[26] Younes MAB. A survey of the most current image encryption and decryption techniques. Int J Adv Res Comput Sci 2019, 10(1): 9.

[27] Lagmiri SN, Elalami N and Elalami J. Color and gray images encryption algorithm using chaotic systems of different dimensions. Int J Comput Sci Network Secur 2018, 18(1): 79–86.

[28] Parameshachari BD, Karappa R, Soyjaudah KS, et al. Partial image encryption algorithm using pixel position manipulation technique: the smart copyback system. In: 2014 4th international conference on artificial intelligence with applications in engineering and technology, Kota Kinabalu, Malaysia, 3–5 December 2014, pp.177–181. New York: IEEE.

[29] Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities. (2017). IGI Global, USA.- P. 301.

[30] Marco Tulio Ram´ırez Torres, Marcela Mej´ıa Carlos, Jose S. Murgu ´ ´ıa Ibarra, Luis Javier Ontanon Garcia. Partial Image Encryption Using Cellular Automata. Computación y Sistemas, Vol. 23, No. 4, 2019, pp. 1575–1582

[31] Ruslan Motornyuk, Andrii Bilan, and Stepan Bilan. Research of Biometric Characteristics of the Shape of the Ears Based on Multi-Coordinate Methods. In book Biometric Identifcation Technologies Based on Modern Data Mining Methods. edited by Stepan Bilan, Mohamed Elhoseny, D. Jude Hemanth pp. 177-194.

[32] Stepan Bilan. Identification of rolling stock of railways based on multi-projection image processing methods. Proceedings of the 7th International Conference "Information Technology and Interactions" (IT&I-2020). Workshops Proceedings Kyiv, Ukraine, December 02-03, 2020. pp. 33-42.

[33] Ruslan Leonidovich Motornyuk, Stepan Bilan. The Moving Object Detection and Research Effects of Noise on Images Based on Cellular Automata With a Hexagonal Coating Form and Radon Transform. Handbook of Research on Intelligent Data Processing and Information Security Systems edited by Stepan Bilan, Saleem Issa Al-Zoubi. pp. 330-359.

[34] Stepan Bilan, Mykola Bilan, Sergii Bilan. Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells.- MATEC Web of Conferences, - Vol. 125,- 02018 (2017), - p. 1-6.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Nashat Al Bdour has written, reviewed, and actively participated in all the publication stages of this manuscript.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author has no conflict of interest to declare that is relevant to the content of this article.