Информационные процессы, Том 25, № 3, 2025, стр. 404–412.

ARTIFICIAL INTELLIGENCE

Method for Automatic Verification of OVI Security Features on Mobile Devices

A. Yu. Popkov, S. A.Usilin, D. P.Nikolaev

[*] *Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia*
[**] *Smart Engines Service, Moscow, Russia*

Recieved October, 1, 2025. Accepted October, 10, 2025

Abstract—In the context of ongoing digitalization and the growing use of remote service channels, the demand for reliable user identification and authentication methods continues to grow. Optically Variable Ink (OVI) is a key technology for protecting printed documents, providing resistance to counterfeiting through complex visual effects. However, existing methods for analyzing and verifying OVI elements typically require specialized equipment, limiting their applicability in mobile and remote scenarios. Moreover, documents containing such security elements often include personal data and are subject to legal or ethical restrictions, making them unsuitable for research. In contrast, banknotes, which commonly incorporate OVI elements but are not subject to such constraints, serve as a practical and accessible source of real-world data. This study proposes a method for verifying the authenticity of OVI security elements using mobile devices. The approach is based on analyzing the position and intensity of maxima in two color channels of digital images. These features are extracted from a sequence of video frames captured by a mobile phone camera while the document is moved under constant lighting conditions. Experimental validation using real-world data from Russian banknotes containing three types of OVI elements demonstrates the effectiveness of the method. A logistic regression model trained on this data achieved average classification accuracies ranging from 84% to 98%, depending on the type of OVI element.

KEYWORDS: optical variable ink, optical variable device, features, computer vision, image processing, document forensics, machine learning.

DOI: 10.53921/18195822_2025_25_3_404

1. INTRODUCTION

In recent decades, the digitalization of the economy has accelerated significantly, leading to the widespread adoption of remote service channels, where the first step typically involves client identification and authentication using an identity document. Mobile devices are commonly employed on the client side to support such services [1, 2]. For reliable identification, it is not sufficient to simply extract personal data; verifying the authenticity of the document itself is equally important.

Since identity documents are a type of secure printed product, they include multiple security elements, some of which can be verified using modern smartphones. These elements include Optical Variable Devices (OVDs) – technologies that produce visual effects through the interaction of materials with incident light, such as color shifts and the appearance of hidden images [3]. A well-known example is holographic elements, frequently used in identification documents [4]. A particularly important class of OVDs involves Optical Variable Ink (OVI), which has been in use since the 1960s [5]. Fig. 1 shows examples of OVI security elements on various secure printed products. OVI contains special opaque components that create characteristic visual effects — iridescence, glare, and color changes depending on the viewing angle (see Fig. 2). These effects

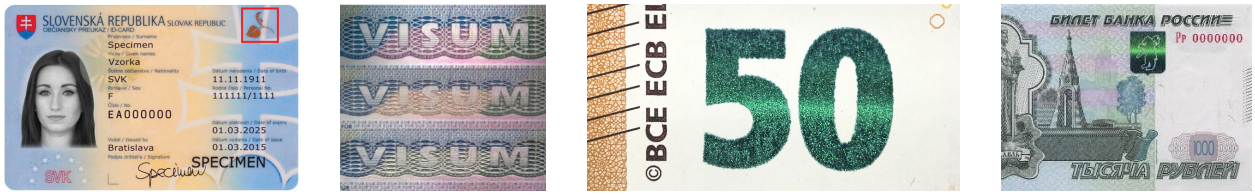

Figure 1. Examples of OVI security elements on various secure printed products (from left to right): 1) Slovak ID Card, 2) EU Visa, 3) OVI element on 50 Euro Banknote, 4) OVI element on Russian 1000 ruble banknote.

can assist in visual authentication, but automated verification typically requires either specialized optical equipment or continuous video capture to reproduce the expected visual changes.

The main advantage of OVI technology lies in its high production cost and limited availability, which make it difficult for counterfeiters. Moreover, OVI is resistant to reproduction using conventional printing, scanning, or standard inks. These properties also pose challenges for the application of artificial intelligence methods, even in research settings.

The object of this study is security elements produced using OVI, which are widely used in banknotes across the world [6]. Unlike other components of security printing, research on OVI remains limited, with most findings being proprietary or embedded in patented technologies. Existing approaches to analyzing OVI-based security elements can be broadly categorized into two classes: physical and information-based.

Physical approaches rely on modeling light reflection and performing spectral analysis. These methods are implemented, for instance, in banknote authentication devices used in banks, ATMs, and vending machines [7,8]. Some studies [9,10] explore the use of multichannel spectrophotometers and reflectance spectroscopy to describe the optical properties of coatings. These efforts primarily aim to validate and confirm declared optical characteristics.

Information-based approaches, on the other hand, utilize features extracted from primary observable properties, such as color, intensity, and texture of reflected light. For example, [11] proposes a method for analyzing holographic elements using the HSV color model, where hue and saturation serve as features. A similar approach is adapted for OVI in [12], showing that the dominant color, determined via clustering methods (e.g., k-means), can be an informative indicator of authenticity. In [13], the variation ranges of color features are analyzed, while [14] proposes a method for detecting security fibers under UV illumination based on pixel brightness gradient analysis.

It is important to note that techniques developed for holographic OVDs are not always applicable to OVI elements, since the latter exhibit different optical behaviors. For instance, holograms typically require the analysis of peak intensity values, whereas OVI relies more on color changes and viewing angle dependency. Because identity documents are directly tied to personal data, their use in research is strictly regulated by law, complicating the development and testing of automated authentication methods. Nevertheless, the advancement of such methods — particularly on mobile or low-cost computing devices — is crucial for improving existing systems and enabling new authentication technologies.

In this context, banknotes hold a unique position: they are both a typical product of security printing and are legally accessible for analysis. Furthermore, banknotes contain a variety of security elements, making them a convenient and diverse research target.

This work proposes a method for automated verification of OVI-based security elements. The focus is on elements produced using OVI, with banknotes serving as an accessible and representative case. Our contributions to this multifaceted problem are as follows:

– We propose indicators of the digital image of an OVI security element that capture its behavior during motion under constant illumination;
– We define a feature extraction procedure from a sequence of such images;
– We introduce and experimentally validate a classification-based method for verifying OVI security elements.

The feasibility and potential effectiveness of the proposed approach are demonstrated through an experimental study using real video data of Russian banknotes in denominations of 1000, 2000, and 5000 rubles.

2. BASELINE DETECTION METHOD OF HOLOGRAPHIC SECURITY ELEMENTS

Due to the fact that holographic security elements belong to the class of optically variable elements, the idea of applying approaches to their recognition and verification to an object of another type, namely, to OVI, seems potentially viable.

We have investigated two methods of hologram detection [11, 17], references to which will be further provided using the `midv-holo` and `holo-base` labels, respectively, adapting them for the objects of the OVI type we are investigating. In [11], a procedure for the extraction and recognition of holographic elements on identification documents is proposed, and in [17] on banknotes, consisting of several successive steps, including those related to the normalization of the carrier object in the frame.

The specificity of light reflection from a holographic element located on a laminated identification document requires the processing of peak intensity values, leading to the loss of color information, and therefore the need for color normalization.

Another feature of the presented task is the need of localization of security elements on the carrier object (in this case, an identification document) when their location relative to other elements is unknown in advance, which leads to the investigation of the entire field of the document being examined.

Our approach, which involves using carrier objects with known locations of security elements, allows us to have a dataset of their sequential images, and therefore we do not need the steps of the procedure associated with their extraction.

The `midv-holo` method of recognition of holographic element is based on the assumption that the hologram reflects light in such a way that its hue and saturation will differ significantly from the surrounding background (along with other elements that do not reflect light). Due to the fact that the identification documents, the study of which is the purpose of the described method, are made of polymeric materials or covered with a film (laminated) with a glossy surface, when they are illuminated, glare occurs on their surface, realized in extreme values of brightness, leading to the loss of color information, and thus requiring separate processing.

The method of recognizing holograms is based on calculating a set of indicators for each image in a sequence of frames, followed by aggregation of these indicators over the entire set of frames, which makes it possible to determine the presence of a holographic element on an object or its absence.

The calculation of the indicators on each image is based on the representation of the image in the HSV color model with the representation of the color space in cylindrical coordinates, where the hue is realized by the angle of the radius vector of saturation.

Next, using a set of consecutive images, aggregated indicators are calculated for each pixel, characterizing the studied carrier object of the security element in the form of maximum saturation, the norm of the sum of color vectors, and the number of processed pixels. The latter are a subset of image pixels that participate in the calculation of the indicators, the remaining pixels are excluded

from this process at the step of processing glare and overexposure described above. Using these indicators, a binary image (mask) is calculated, based on the proportion of significant pixels in which a decision is made on the presence or absence of a hologram.

The `holo-base` method is based on the observation that the hue distribution of a holographic security element is significantly wider than that of the surrounding background. It is proposed to estimate the width of the distribution using an analogue of the interquartile range (IQR), after having previously performed a certain image processing such as filtering too dark areas.

In both methods, the hyperparameters are implemented as various thresholds, which can be used to fit them within any machine learning procedure. Given that we do not need to select a security element on the carrier object, but need to verify it, we adapted the described methods to the OVI security elements we studied by introducing a hyperparameter of the share of the security element area in the area of the entire image. To configure the hyperparameters, we set the intervals of their values; we chose the interval of the area share parameter to be 70-95%. Then we optimized them by enumerating the parameter grid within the procedure of randomly dividing the training data into training and test data and calculating the maximum accuracy on the test data. To obtain average quality estimates, we repeated this procedure 10 times.

As a result of applying the above methods to the data set used by us in this work, the following results were obtained (see Table 1), showing the lack of effectiveness of their application to OVI security elements, which emphasizes the relevance of developing specialized methods and approaches to their analysis.

Table 1. Results of baseline methods for holographic security elements recognition.

Type	`midv-holo`	`holo-base`
`1000r_A`	0.43	0.52
`2000r_A`	0.33	0.66
`5000r_B`	0.53	0.46

3. PROPOSED METHOD FOR AUTHENCITY VERIFICATION OF THE OVI SECURITY ELEMENT

As noted in the Introduction, OVI elements exhibit a distinctive property: their appearance changes depending on lighting conditions and the viewing angle. Fig. 2 shows several frames of a security element on one of the analyzed banknote types, illustrating the dynamic nature of its visual behavior.

Figure 2. Observable dynamics of the security element during motion under constant illumination.

To isolate the security element for further analysis, a sequence of frames must first be extracted from the input video. Then, for each frame, the object containing the security element is normalized, and the element itself is localized within the normalized object. This multi-stage process requires the application of several techniques, including keypoint detection, restoration of perspective transformation, and image stabilization [15, 16]. As the implementation of this process lies

beyond the scope of this work, we assume as input a sequence of preprocessed, normalized images of the security element captured during motion of the carrier (e.g., a banknote) within the video frame.

Thus, in this study, the security element is represented by a set of consecutive images captured under conditions that reveal its key property — optical variability. The proposed verification procedure, illustrated in Fig. 3, is based on binary classification. It involves a sequence of steps aimed at determining whether the observed element corresponds to a genuine OVI security element.

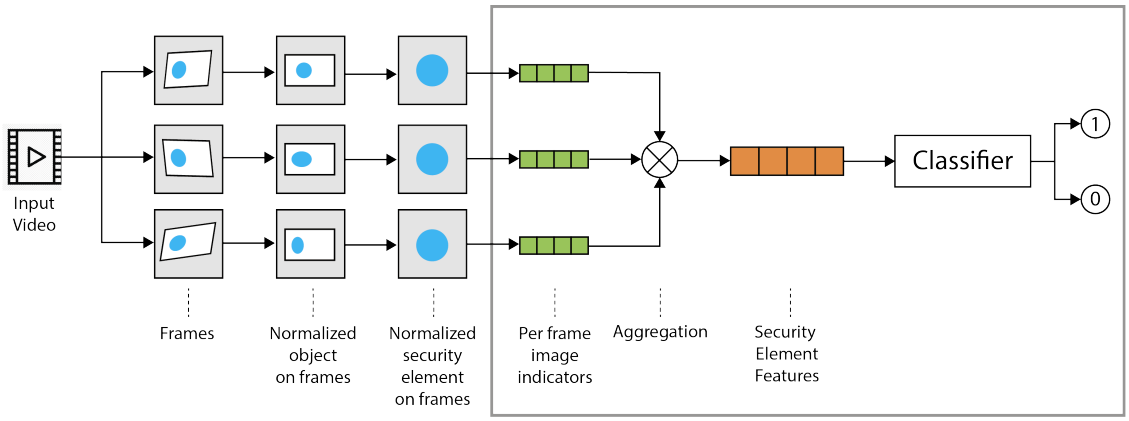

Figure 3. Security element verification procedure.

The security element submitted for verification is characterized by a sequence of images captured as it moves within the frame.

For each image in the sequence, image indicators are computed. These indicators are then aggregated across the entire sequence to form a unified object features, which is fed into a classifier. The classifier produces a binary decision — indicating whether or not the analyzed object corresponds to an OVI-based security element.

3.1. Image Indicators

Visual analysis of the dynamics of light reflected from the security element (see Fig. 2) suggests that this behavior can be quantitatively assessed using the saturation (S) and value (V) components of the HSV color model.

Let $S(x, y)$ and $V(x, y)$ denote the saturation and value of a pixel at coordinates (x, y), and let M_S and M_V represent the median saturation and value across the image, respectively. We define the horizontal and vertical coordinates of the relative maxima for the saturation and value as:

$$x_S^*(y) = arg\max_x \frac{S(x,y)}{M_S} \quad y_S^*(x) = arg\max_y \frac{S(x,y)}{M_S},$$
$$x_V^*(y) = arg\max_x \frac{V(x,y)}{M_V} \quad y_V^*(x) = arg\max_y \frac{V(x,y)}{M_V}.$$

Fig. 4 shows images of security elements of three different types, with points indicating the positions of relative maxima for the value component. Maxima along the horizontal axis x are marked in blue, while those along the vertical axis y are marked in green. The spread in these maxima positions is visibly significant.

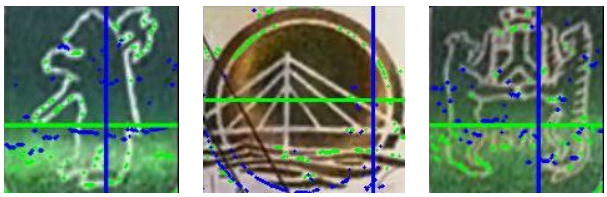

Figure 4. Positions of relative value maxima for security elements of different types.

Averaging these indices, we obtain the indicators of the position of the relative maximum of saturation and value:

$$S_x = \frac{1}{n}\sum_y x_S^*(y), \quad S_y = \frac{1}{m}\sum_x y_S^*(x), \tag{1}$$

$$V_x = \frac{1}{n}\sum_y x_V^*(y), \quad V_y = \frac{1}{m}\sum_x y_V^*(x), \tag{2}$$

where n and m are the image dimensions in pixels along the vertical and horizontal axes, respectively. These indicators are shown in Fig. 4 as vertical and horizontal lines in the corresponding colors. We also define the relative maxima of saturation and value:

$$S_{val} = \max\frac{S(x,y)}{M_S}, \quad V_{val} = \max\frac{V(x,y)}{M_V}. \tag{3}$$

Thus, each individual image of the security element is characterized by two types of indicators: the *position* of the relative saturation and intensity (value), as defined in (1) and (2); and the *value* of these relative maxima, as defined in (3). The set of these indicators, computed across the image sequence, forms the *observed data* used to analyze the dynamic behavior of light reflection from the security element.

3.2. Features of the Security Element

Based on the image indicators described above for the saturation and value components, we represent them as vectors: $S = (S_x, S_y, S_{val})$, $V = (V_x, V_y, V_{val})$. Given a sequence of images for each specific security element, we compute empirical statistical characteristics for each component of the vectors S and V. In particular, we calculate the mean (denoted by the subscript avg), standard deviation (std), minimum (min), and maximum (max) bounds of variation in the respective channels. These indicators are treated as potential *features* of the element.

However, not all potential features are equally informative for classification, and the high dimensionality of the resulting feature space can reduce the generalization ability of classifiers trained on limited data. To address this, we perform feature selection using a specific criterion. For this purpose, we employ a logistic regression model and evaluate several subsets of features drawn from the full set of candidates. The model is trained on all available data for each element type to identify the subset that yields the highest classification accuracy. As previously noted, the variation in image indicators across consecutive frames is often substantial. For this reason, we focus on feature combinations based on standard deviations, which capture the variability of the element's response. These features are aggregated from the saturation and value indicators of individual frames. Each element is therefore described by six numerical features based on standard deviation: $S^{std} = (S_x^{std}, S_y^{std}, S_{val}^{std})$, $V^{std} = (V_x^{std}, V_y^{std}, V_{val}^{std})$. From these, we select the minimal subset of features that provides the best classification performance (in terms of accuracy) for each specific element type.

3.3. Classification

The process of computing image-level indicators, followed by the extraction of features for each security element, enables the construction of a feature space specific to a given type of security element. As previously noted, the selected feature set may vary depending on the configuration of the security element. Classification is then performed using a logistic regression model, with its parameters optimized via cross-validation to ensure generalization and improve prediction accuracy

4. EXPERIMENTAL STUDY

Experiments were conducted using Python 3.12 on a Windows x64 platform with the following libraries: OpenCV 4.11, NumPy 2.2.2, and scikit-learn 1.6.1. The `LogisticRegression` implementation from scikit-learn was used for training the classification model with default parameter settings.

4.1. Data

The experimental study utilized a dataset available for free download at [`ftp://smartengines.com/rus_banknotes_ovi`] comprising three types of original Russian banknotes and their copies produced via laser color copying. The main characteristics of the dataset are summarized in Table 2. Each element in the dataset is represented by a video recording of a banknote captured using an Apple iPhone 15 smartphone under standard lighting conditions and default camera settings. From each video, a sequence of 10 JPEG frames was extracted, containing normalized images of the security element. Frame extraction was performed using the OpenCV library with a step of 10 frames. No additional image preprocessing was applied prior to analysis.

Table 2. Dataset characteristics.

Type	Number of objects	Number of originals	Number of copies	Class distribution in %
`1000r_A`	24	13	11	55/45
`2000r_A`	14	6	8	43/57
`5000r_B`	16	8	8	50/50

4.2. Feature Selection

For feature selection, we considered multiple combinations of *features* based on the standard deviations of the image indicators. For each object type in the dataset, a logistic regression model was trained, and the feature set yielding the highest classification accuracy was selected. The final selected feature sets are summarized in Table 3. It is important to note that different feature sets were required for different object types due to variations in the configuration of the security elements. In particular, for security elements of the `2000r_A` type, the color dynamics during motion were pronounced in both the vertical and horizontal directions, resulting in significant variation in the corresponding image indicators.

Table 3. Selected features.

Type	Features
`1000r_A`	V_y^{std}, V_{val}^{std}
`2000r_A`	S_x^{std}, S_y^{std}, V_x^{std}, V_y^{std}
`5000r_B`	V_y^{std}, V_{val}^{std}

4.3. Classification

The classification experiments were conducted in the corresponding feature space for each object type by randomly splitting the dataset into a training set (referred to as train) and a test set (test) in a 70 : 30 ratio. Randomization (shuffling) was applied at each repetition of the experiment. The performance metrics were averaged over 100 trials, resulting in an estimate of the mean classification accuracy on the test set.

The results, presented in Table 4, include the number of elements per class and the corresponding average accuracy values.

Table 4. Classification results.

Type	N_train	N_test	Mean Accuracy
1000r_A	17	7	0.91
2000r_A	10	4	0.84
5000r_B	11	5	0.98

The results demonstrate that the classification performance varies significantly across different object types. This variation is primarily attributed to differences in the configuration and structure of the security elements. Specifically: elements of type 1000r_A and 5000r_B generally exhibit uniform coloration, with most noticeable color changes occurring in the vertical direction; in contrast, elements of type 2000r_A have a complex circular design, with color dynamics present in both horizontal and vertical directions. Additionally, the behavior of saturation and value differs among the element types. It is also important to note that no additional image preprocessing — such as noise reduction, color normalization, or sharpening — was applied. The potential impact of such preprocessing techniques on classification accuracy remains a subject for future investigation.

5. CONCLUSION

This work presents a method for verifying the authenticity of Optically Variable Ink (OVI) security elements based on the analysis of digital images captured using a mobile device. The proposed approach is centered on analyzing the dynamics of light reflection from the security element during its motion under constant illumination, with the extraction of features related to the position and value of local maxima in two image channels. Classification is then performed using a logistic regression model. Experimental evaluation conducted on three types of OVI security elements found on Russian banknotes demonstrated the potential effectiveness of the method, achieving average classification accuracy ranging from 84% to 98%, depending on the type of security element.

Future research will focus on evaluating the method's robustness under varying conditions, such as changes in illumination, banknote motion characteristics within the frame, and environmental noise. Further plans include expanding the dataset and exploring the impact of preprocessing techniques such as noise reduction, color normalization, and image enhancement on overall classification performance.

REFERENCES

1. V. V. Arlazarov, K. Bulatov, T. Chernov, V. L. Arlazarov. MIDV-500: a dataset for identity document analysis and recognition on mobile devices in video stream. Computer Optics, 2019, Vol. 43, No. 5, pp. 818-824, https://doi.org/10.18287/2412-6179-2019-43-5-818-824.

2. Y. S. Chernyshova, M. A. Aliev, A. V. Sheshkus. Optical font recognition of images captured with mobile devices and its application for detecting identity documents forgery // Proceedings ISA RAS, 2018, Vol. 68, pp. 183-191, http://doi.org/10.14357/20790279180521.

3. J. W. Mercer. Evaluation of optical security features in ID documents, currency, and stamps, Proc. SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, (19 April 2002); https://doi.org/10.1117/12.462725.

4. D. V. Polevoy, E. I. Panfilova, and D. P. Nikolaev. White balance correction for detection of holograms in color images of black and white photographs // Informatsionnye Tehnologyi i Vycheslitelnie Sistemy, 2021, No. 3, pp. 82-95, http://doi.org/10.14357/20718632210308.

5. PRADO — Public Register of Authentic Identity and Travel Documents Online — Glossary https://www.consilium.europa.eu/prado/en/prado-glossary/prado-glossary.pdf (Accessed: 04 June 2025)

6. I. Lancaster, A. Mitchell. The growth of optically variable features on banknotes // Proceedings Volume 5310, Optical Security and Counterfeit Deterrence Techniques V; (2004) https://doi.org/10.1117/12.549893.

7. P. G. Coombs, T. Markantes. Improved verification methods for OVI security ink // Proc. SPIE 3973, Optical Security and Counterfeit Deterrence Techniques III, 2000, https://doi.org/10.1117/12.382200.

8. P. G. Coombs, S. M. McCaffery, and T. Markantes. Advanced verification methods for OVI security ink // Proc. SPIE 6075, Optical Security and Counterfeit Deterrence Techniques VI, 60750I (9 February 2006); https://doi.org/10.1117/12.652451.

9. Z. Wei, Y. Liu, Y. Shen, X. Gong, X. Li, and M. Huang. Evaluation of Color Measurement Geometries for Optically Variable Inks. In: Song, H., Xu, M., Yang, L., Zhang, L., Yan, S. (eds) Innovative Technologies for Printing, Packaging and Digital Media, CACPP 2023. Lecture Notes in Electrical Engineering, vol 1144, Springer, Singapore. https://doi.org/10.1007/978-981-99-9955-2_7.

10. O. Gómez, E. Perales, E. Chorro, F. J. Burgos, V. Viqueira, M. Vilaseca, F. M. Martínez-Verdú, and J. Pujol. Visual and instrumental assessments of color differences in automotive coatings. Color Res. Appl., 2016, Vol. 41, pp. 384-391, https://doi.org/10.1002/col.21964.

11. L. I. Koliaskina, E. V. Emelianova, D. V. Tropin, V. V. Popov, K. B. Bulatov, D. P. Nikolaev, and V. V. Arlazarov. MIDV-Holo: A Dataset for ID Document Hologram Detection in a Video Stream. In Document Analysis and Recognition - ICDAR 2023: 17th International Conference, San José, CA, USA, August 21–26, 2023, Proceedings, Part III. Springer-Verlag, Berlin, Heidelberg, 486–503. https://doi.org/10.1007/978-3-031-41682-8_30.

12. L. Piatriková, P. Tarábek, and I. Cimrák. Digital Verification of Optically Variable Ink Feature on Identity Cards // 33rd Conference of Open Innovations Association (FRUCT), Zilina, Slovakia, 2023, pp. 210-218, https://doi.org/10.23919/FRUCT58615.2023.10142989.

13. Z. Ahmed, S. Yasmin, M. N. Islam, and R. U. Ahmed. Image processing based Feature extraction of Bangladeshi banknotes // The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014), Dhaka, Bangladesh, 2014, pp. 1-8, https://doi.org/10.1109/SKIMA.2014.7083521.

14. I. A. Kunina, M. A. Aliev, N. V. Arlazarov, and D. V. Polevoy. A method of fluorescent fibers detection on identity documents under ultraviolet light // Proc. SPIE 11433, Twelfth International Conference on Machine Vision (ICMV 2019), 114330D (31 January 2020); https://doi.org/10.1117/12.2558080.

15. K.B. Bulatov, E.V. Emelianova, D.V. Tropin, N.S. Skoryukina, Y.S. Chernyshova, A.V. Sheshkus, S.A. Usilin, Z. Ming, J.-C. Burie, M. M. Luqman, V.V. Arlazarov. MIDV-2020: A Comprehensive Benchmark Dataset for Identity Document Analysis // Computer Optics, 2022, V. 46, No. 2, pp. 252-270, http://doi.org/10.18287/2412-6179-CO-1006.

16. N. S. Skoryukina, D. V. Tropin, J. A. Shemiakina, V. V. Arlazarov. Document Localization and Classification As Stages of a Document Recognition System // Pattern Recognition and Image Analysis, 2023, V. 33, No. 4, pp. 699-716, https://doi.org/10.1134/S1054661823040430.

17. How to detect a hologram with OpenCV, https://ai-facets.org/tag/opencv/ (Accessed: 04 June 2025).