# Digital Verification of Optically Variable Ink Feature on Identity Cards

Lucia Piatriková, Peter Tarábek, Ivan Cimrák
University of Žilina
Žilina, Slovakia
Lucia.Piatrikova, Peter.Tarabek, Ivan.Cimrak@fri.uniza.sk

***Abstract*—Digital identity verification is a new trend that allows clients to access services and products remotely, simplifies the interaction between client and institution, and saves their expenses. Digital verification suffers many security risks. The system must be able to reveal counterfeit identity cards. We propose a procedure to verify ID cards based on an analysis of the Optically Variable Ink (OVI) security feature. OVI is a type of ink whose colour varies with rotation or changes in the observer or light source position. The proposed method can detect an ID card and an OVI security feature on video frames. OVI visual characteristics are analysed, and we provide methods for their visual verification. We make several recommendations and suggestions for solving various partial problems related to visual OVI verification. Proposed methods can reveal counterfeit ID card in a video by analysing the OVI security feature with an accuracy of 82.82% but with some limitations.**

## I. Introduction

Digital identity verification is a new trend in banking, telecommunications and other services. It substitutes personal identification and verification of a client by company employees and allows the client to use its services without visiting an office. Generally, it simplifies the interaction between the client and the institution and saves their expenses.

Digital identity verification suffers security risks because part of the process is in an uncontrolled environment in the hands of a client. The system must be able to detect forgery that would be obvious in personal verification, e.g., a printed ID card.

The essential part of the verification is the inspection of ID card security features. Digital verification of security features can supplement a complex ID card verification system and increase its robustness.

Other works mainly focus on the digital verification of holograms. Reference [1] proposes an interactive application for mobile devices which can recognize documents using the SURF algorithm for keypoint detection in combination with clustering, and interactively verify view-dependent hologram. Depending on the current view of the document, the application presents a stored image of the element. It requires the use of a flashlight which dominates other light sources. Another approach to hologram verification is by [2]. They developed a portable illumination module to acquire images of holograms by mobile devices. A convolutional neural network is used to represent Euro banknote holograms and cosine distance measures dissimilarity. Reference [3] proposes an end-to-end

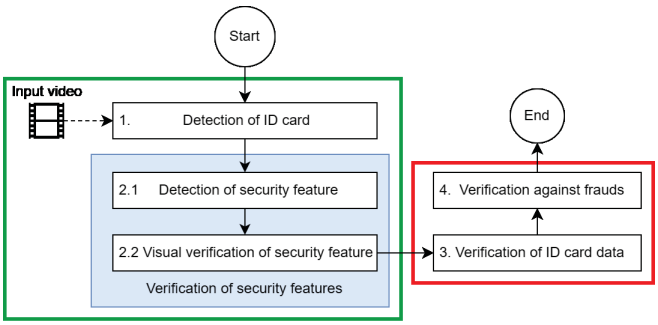



Fig. 1. Digital verification of ID card

hologram verification system which uses the CNN methods. They generated fake holograms with the use of the GANs. Another work [4] proposes a banknote recognition system based on computer vision. It applies the SURF algorithm for keypoint detection to real-life videos with banknotes.

This paper is devoted to the analysis and digital verification of the security feature with Optically Variable Ink (OVI) on the Slovak ID card. To the best of our belief, the authors are not aware of any previous work dedicated specifically to the OVI security feature. In the paper, we analyse possible approaches or methods for OVI verification. We can find ID cards in video frames and then the OVI feature on the particular detected ID card. For OVI verification, we utilize different visual characteristics of detected OVI features.

Several ID cards from foreign countries also contain the OVI security feature, which can be different in colour and shape, but the overall characteristics are identical. Therefore, all proposed methods after a little modification can be applied to foreign ID cards with the OVI feature.

This section continues with a description of a possible digital verification procedure for the ID card and an analysis of the ID card security features, emphasising the OVI feature in connection with digital verification. In section II, we introduce the proposed OVI feature verification procedure and explain the proposed methods, which can be classified into three categories, i.e., the detection of ID card, the detection of OVI security feature, and the verification of OVI visual properties. In section III are summarized results of the OVI feature verification procedure. The paper ends with the conclusion in section IV.


Fig. 2. Slovak ID card with marked OVI

### A. Digital verification procedure of ID card

An original ID card has all the security features, and all the written information is authentic. All these aspects must be verified to consider an ID card real. Fig. 1 illustrates the digital verification procedure of an ID card. If all steps are successfully verified, the ID card is considered real.

The input to the digital verification of an ID card is a video recorded by a client on a mobile phone or arbitrary smart device. We assume the data authenticity at the sensor level, i.e., the input data are original and transferred through a secure channel. The video captures the entire ID card, which changes its position to the camera and the light source. The camera flash is expected as the primary light source. The movement of the ID card or the camera can be completely random, but a sufficient colour change of the OVI feature must be captured in the video.

In the first step, we search for the ID card in the video frames, and then its security features are verified. The security feature's presence and the required properties' satisfaction are checked. The verification concerns the placement of the security feature in the context of the ID card.

The next step is the verification of the ID card data, i.e., a person's existence, facial biometrics, and the validity of the personal data listed on the ID card by comparing it with the external database. The data are read using the OCR method. Their consistency, corresponding type of document, identification number, photo, etc., are verified. And the last step is the verification against different types of fraud, e.g., pasting an image over. For this phase, it is convenient to incorporate machine learning models.

In this paper, we focus only on the verification of the OVI security feature. In Fig. 1, the green colour denotes the points further discussed in the paper, specifically steps 1 and 2 in connection with the OVI security feature. The complete verification procedure described in this section is only a suggestion that incorporates the OVI verification.

### B. ID card security features

Security features prevent ID cards from being falsified. Security features of the Slovak ID card are described in detail in official documents [5], [6], [7]. PRADO - Public

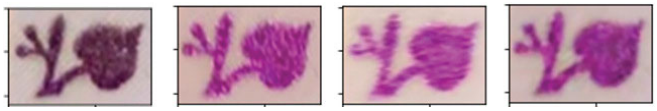


Fig. 3. OVI colours at different positions to the camera

Register of Authentic identity and travel Documents Online [8] summarizes European identity cards and their security features together with their technical details.

Each security feature is unique and has specific properties, but not all of them can be verified visually. From an image or a video, we can check only the visual properties of security features, disregarding other properties, e.g, tactile properties.

Recording the ID card has certain limitations that make it difficult to check some security features. The analysis of miniature security features requires high-quality and high-resolution photography, which is a challenging prerequisite under normal conditions, assuming the system will be used by users with arbitrary cameras. That applies to the background security feature, where smooth colour transitions need to be verified, and to the fine guilloche protective underprint. Another miniature feature is the microtext. Even in physical verification, these features require a magnifying tool.

Another security feature, the fluorescent overprint, is only visible under UV light and not under normal lighting. Thus, security features with this property are hardly possible to be checked under normal conditions.

Relief embossing is a tactile and colourless security feature, but it is visible under normal lighting. Since it consists of microtext, the visual verification requires high-quality photography.

The ID cards carry sensitive personal data that must be protected. Some security features are located near personal data or overlap with them. It complicates their detection and validation. During the design of the whole digital verification system, the protection of personal data must be considered.

### C. OVI security feature

Optically Variable Ink (OVI) is a security feature whose visual display of information depends on the current observation and lighting conditions. Especially, OVI is a type of ink that consists of microscopic pigments acting as interference filters. Therefore, it changes its hue when the angle with an observer, the angle with a light source, or the lighting is modified, thus preventing the ID card from being copied in colour [8]. In Fig. 3, the OVI feature is illustrated by changing its position to the camera, which leads to different observed colours.

OVI is visually characterized by its colour and shape in the particular observing position. The visual change in the OVI colour is a convenient characteristic potentially adaptable in visual detection and verification. In counterfeit ID cards, OVI colour was captured in the specific situation and permanently remains constant.

In this paper, we focus on the OVI security feature in the Slovak ID cards located on the front side in the upper right corner, as denoted in Fig. 2. Currently, two ID card versions

are valid, both having the OVI symbol of the shape of a linden leaf and their colours ranging from purple to green. OVI does not collide with any personal data, thus preserving a person's anonymity. For this reason, OVI appearance is independent of the particular ID card, thus is easier to be detected and analysed.

## II. Proposed procedure

In the following section, we propose the OVI feature verification procedure and the methods in detail. We categorize methods into three categories, namely methods for the detection of ID card, the detection of OVI security feature, and the verification of OVI visual properties.

The verification procedure of the OVI security feature is proposed as follows. The input to the method is a sequence of video frames with the ID card captured in different positions to the image sensor. The OVI detection is performed sequentially for each frame. After the entire input sequence passed the detection, the second part verifies the OVI visual properties.

In the first step, the detector searches for the ID card in the scene of the currently analysed image. The SIFT algorithm detects the ID card and uses the predefined normalized ID card as a reference image. A transformation matrix is calculated based on the matched keypoints and used for ID card normalization. The transformation matrix stores the information related to the ID card position in the original image and thus is saved for the colour analysis step.

For each normalized ID card, the upper right corner is cut out. Template Matching does the OVI cut and SIFT algorithm checks the symbol shape. The resulting OVI image cuts continue to the next verification phase.

Approaching the visual verification part, the first property being verified is glittering. For each OVI image cut, the edge score is calculated. If it is below the predefined threshold value, the image cut is considered incorrect and excluded from further analysis.

In the final step, the dominant colour is calculated for OVI image cuts, which are considered to be correctly detected. Then, the verification of a change in the colour of the OVI feature is performed. We check the change in brightness, i.e., the V component of the dominant colours stored in the HSV model. The minimum and maximum value of the V component is found in the whole video. If the captured difference is above the predefined threshold, the colour change is considered to be verified. And similarly, the OVI security feature and ID card are marked as authentic. The proposed procedure is illustrated in Fig. 4.

### A. Detection of ID card

Detection of the ID card in video frames is the first fundamental step in the ID card verification process. In connection with the OVI verification, it ensures that the security feature is placed on the ID card and in the correct position. Furthermore, the detected ID card can be taken as input into the analysis of other security features and the verification of personal data.

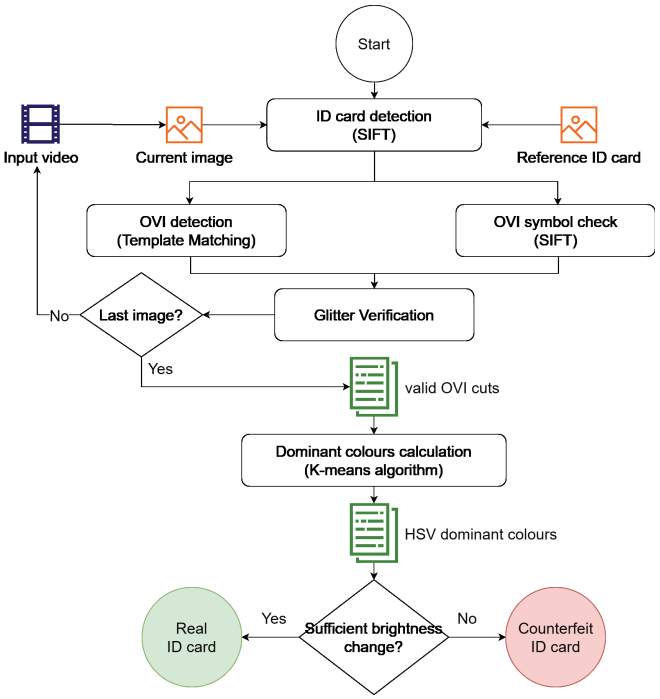



Fig. 4. Proposed procedure

Algorithm SIFT [9] for keypoint detection we find the most rewarding for the detection of the ID card. SIFT algorithm extracts keypoints from an image. Keypoint represents a local image feature. The algorithm is invariant to rotation and image scaling and is partially invariant to affine distortion, the addition of noise and illumination change.

SIFT algorithm finds the keypoints of a currently analysed image and then compares them to the keypoints of a template image. The template image is a normalized ID card, meaning it is upright in front of the camera sensor and without any background. If a sufficient number of keypoints matches, the ID card is successfully found in the image.

From the matched keypoints is calculated a homography. The homography is a transformation matrix, that describes the position of the analysed ID card image to the template ID image, along with the position of the camera sensor. Then, homography is used for ID card normalization, as we can be seen in Fig. 5. The normalized ID card image with a transformation matrix is the input to the consecutive ID verification process.

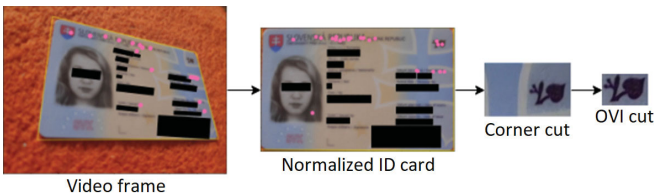



Fig. 5. Detection of OVI security feature

### B. Detection of OVI security feature

Detection of the OVI security feature is the second step in the OVI verification process. Only if the OVI feature is found, we can verify its visual characteristics.

From a detected and normalized ID card, we cut out the upper right corner to focus on the relevant part of the ID card. This larger image cut is the input to our OVI detection method. We can not cut the OVI feature directly from the ID card because normalization is not perfect. Thus OVI feature is not necessarily at the expected position. These steps are illustrated in Fig. 5.

The proposed OVI detection method is a combination of colour-oriented Template Matching and shape-oriented SIFT algorithm. Firstly, sequentially for each video frame, Template Matching makes the candidate image cut with the OVI feature possibly on it. Multiple OVI templates must be used because multiple types of ID cards with different colours and shapes of symbols may be valid at the same time.

In Template Matching, we use the Square Difference metric from [10] for the score calculation defined as follows:

$$R(x,y) = \sum_{x',y'} \left(T(x',y') - I(x+x',y+y')\right)^2 \qquad (1)$$

where $R(x,y)$ is output matrix with position scores, $T$ is template image and $I$ is analysed image.

Template Matching is not invariant to image rotation or scaling. This shortage is solved thanks to the fact that all normalized ID cards have the same scale. Another drawback is sensitivity to lighting conditions. The matching score depends on the colour of the OVI feature, and the method always returns the position with the lowest distance score, either if the OVI was not found. For these reasons, we combine Template Matching with keypoint detection.

Keypoint detection of the OVI feature is more complicated than the detection of ID cards due to the colour change of the OVI feature, specifically from dark to light and vice-versa, and OVI glitters. It is not an appropriate method to detect the OVI feature independently. However, if an insufficient number of keypoints is matched, we know that the OVI feature is not detected. Thus it can supplement a colour-oriented Template Matching.

For each type of OVI symbol, SIFT algorithm for keypoint detection checks the symbol shape in the image cuts made by Template Matching. It is not successful on cuts from all video frames but at least on some of them. If the same OVI feature symbol is found on a sufficient number of frames, the given symbol is definitely present on the analysed ID card. Thus we can use it as a symbol checker to exclude the candidates for which Template Matching based its decision on the wrong type of OVI symbol. The sequence with detected image cuts of the OVI feature steps into the visual verification part.

### C. Visual verification of OVI security feature

Visual verification of OVI is a complex problem with different aspects. We propose three visual characteristics of the OVI feature that we suggest to be verified. The first characteristic is the glittering of OVI pigments which can detect wrong image cuts with absenting OVI. The second aspect is the OVI colour with respect to the ID card position in an image. Finally, the third characteristic is the OVI colour change captured in the video to ensure that the user moves the ID card.

The second and third characteristics are complementary. Without the check of the OVI colour with respect to the ID position, someone can deceive our system by putting something of different colour in front of the OVI symbol, causing a significant colour change. On the other hand, when the user does not move the counterfeit ID card in the video, its position remains constant. The OVI colour can match this particular position, and the OVI feature will be considered mistakenly real if the colour change verification step is not implemented. For these reasons, all three OVI characteristics are relevant and needed to be verified. In this paper, we focus only on two of discussed visual properties, namely glittering and change in OVI colour.

*1) Effect of photographing on the visual properties of OVI feature:* The analysis of the visual properties of the OVI feature is complicated by the high variance in lighting conditions, that affect the observed colour. Analysing all possible combinations of lighting and image sensor properties along with camera settings is challenging. In this subsection, we summarize the main factors influencing the visual properties of the OVI feature in photography.

Before photographing, the light source properties significantly influence the colour of the OVI. The observed colour depends on the colour temperature of the light source [11]. The colour temperature of sunlight changes during the day, but the temperature of the camera flash is mostly constant. If the white colour is not balanced in the picture, i.e., the temperature of the light source deviates from the neutral white, the colour of the OVI also deviates [12]. In Fig. 6, images of the OVI feature are taken at the same position but illuminated by light sources with different temperatures, causing the OVI colour to be different for each light source.

The prerequisite for the digital verification of the OVI authenticity is the quality and resolution of the photography. Too much light captured by the image sensor, e.g., caused by light reflection from the smooth surface of the ID card, can cause distortion and lead to an overexposed image. The brightness of the OVI colour can be adjusted by the exposure settings, especially shutter speed, aperture, ISO, and the dynamic range of the image sensor in connection with the ID card

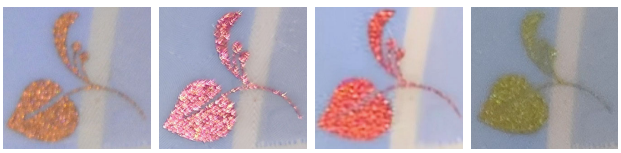


Fig. 6. OVI colour depends on light source temperature

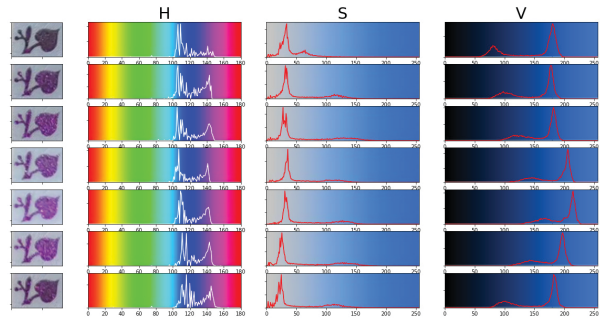
background. Camera image sensor properties, e.g., sensor size or resolution, affect the OVI colour, too.

The analysed video should capture a broad spectrum of OVI colours. The OVI colour change is caused by the change in the position of OVI to a light source, or an observer. In the OVI digital verification, we can locate the position of the image sensor concerning the ID card, but not the light source position. For this reason, the proposed verification procedure requires a camera flash as a primary light source, causing the sensor and light source positions to be almost equal. And therefore, we can consider the relationship between the position and the colour of the OVI feature. But as a consequence, this solution is less robust.

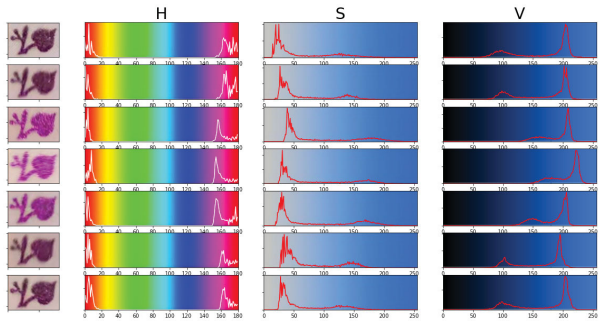
*2) Colour analysis of OVI:* We analysed the relationship between the colour and position of the OVI, assuming that the primary light source is a camera flash. For the analysis, we created several series of images by horizontally rotating the ID card from the left to the right and making the OVI image cuts.

The HSV colour model separates hue information from saturation and brightness. The histograms of HSV colour channels of two OVI series with little different lighting conditions are in Fig. 7. The major shift can be observed in the H component, but the histograms of S and V are similar. We conclude that the change in lighting is reflected mainly by the chromatic H component, for which is colour spectrum skewed. Components S and V can thus be compared among series, even without colour normalization.

Fig. 8 shows heatmaps of HSV components of two OVI series. According to the heatmaps, again components S and V are comparable. The glittering and colour change of the OVI feature is mainly observable in the V component, which has higher values for more glittering and brighter colours.




(a) Series 1




(b) Series 2

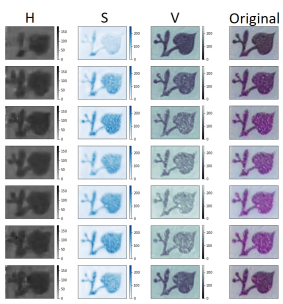
Fig. 7. HSV histograms of OVI series

The proposed methods work with OVI colour represented in the HSV colour model, focusing on the S and V components, which are less sensitive to the lighting conditions and white balance of the image. Verification of component H is a more complex problem, where H component normalization is probably needed.

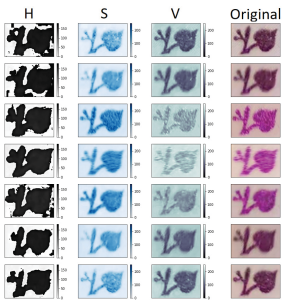
*3) Colour representation:* OVI colour in the image cut can be represented at different levels of simplification. The simplest representation is a dominant colour. More informative is the histogram of colour channels. In the case of these two representations, i.e., the dominant colour and the histogram, the spatial information is not included. More information is involved in the 2D representation of colour components using a heatmap and when the whole image cut is used. It is also convenient to consider a more sophisticated transformation of the input images by applying some image signal processing methods.

In the proposed verification process, we use dominant colour representation. The dominant colour is computed by clustering, specifically the K-means algorithm. Input to the algorithm is an OVI image cut in the RGB colour model. The cluster centre is calculated as the average colour of pixels assigned to the cluster, and each centre corresponds to one dominant colour of the image. In the colour verification, we use the dominant colour converted to the HSV colour model.

OVI image cut colours can be split into two groups, i.e., background colours and OVI colours. The K-means algorithm requires a count of clusters to be defined in advance, thus we can specify the desired number of dominant colours. We experimented with a different number of dominant colours. In Fig. 9 are two OVI feature images. For each, dominant colours are computed for the 2, 3, and 5 clusters. Below the dominant colour is its percentage representation in the image. We conclude that two clusters are enough to separate the background from the OVI colour. OVI colour commonly covers fewer pixels in the image, and the background colour has a higher value of the blue colour channel B in the RGB model.




(a) Series 1




(b) Series 2

Fig. 8. HSV heatmaps of OVI series

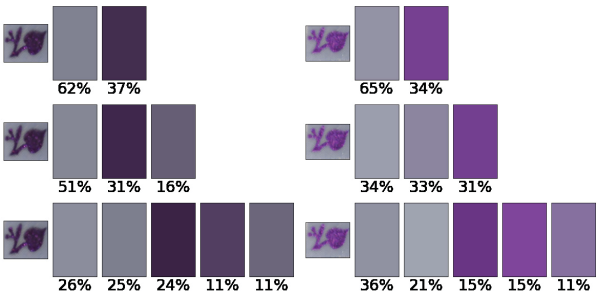



Fig. 9. Dominant colours for a different number of clusters

*4) Glitter verification:* OVI glittering is due to microscopic pigments which OVI is made from. It can also be captured on a counterfeit ID card, so it is integrated into the detection of incorrect image cuts with absenting OVI, rather than revealing the counterfeit.

In the proposed verification process, for glitter verification, we adopt edge detection. In Fig. 10 are outputs of three edge detection filters applied to the OVI image cut. As we can observe, glittering is captured as a high number of short edges in an image and could be used for glittering quantification.

To quantify glittering, we define the edge score calculated from the output of the Laplace filter applied to the OVI image cut. The score can be calculated using the following formula:

$$\text{score}(X) = \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} |X_{i,j} - X_{i+1,j+1}| \qquad (2)$$

where $X$ is an output of the Laplace filter applied to the OVI image cut with the size of $M \times N$.

For the next steps of OVI colour verification is crucial to keep only the correct OVI image cuts at the correct positions. For this reason, we incorporate glittering verification into the OVI detection part. We can summarize the proposed OVI detection as follows. The inputs are normalized ID cards from the ID card detection step. The Template Matching makes OVI image cuts, and SIFT algorithm does the symbol checking, as explained in section II-B. In the end, the edge score is calculated for each OVI image cut, and cuts with low edge scores are excluded from further analysis.

An alternative to edge detection is checking the variety of captured colours. In Fig. 7, we can observe that colour component H does not have two peaks, one for a background and one for an OVI, but a higher number of smaller peaks indicating a high number of different colours captured in the small area. It is because OVI colour pigments reflect a broad colour spectrum. This problem can be formulated as searching for a wide enough range of colours captured in the image, i.e., a sufficient number of histogram peaks. This approach is not included in our verification process, but we suggest it for deeper exploration.

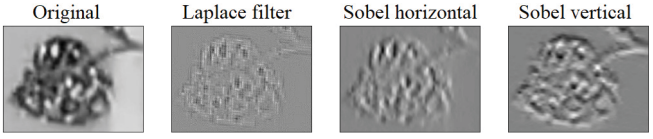



Fig. 10. Edge filters applied to OVI feature

*5) Verification of captured change in OVI colour:* Verification of change in OVI colour can detect the two following situations. Firstly, the OVI colour is not changing due to a counterfeit ID card, and secondly, a user is not moving the ID card, thus its colour remains constant. But even in the case of the counterfeit ID card, small changes in the dominant colour caused by lighting, sensor properties, or light reflection can be captured in the video. Therefore, it is necessary to verify a sufficient change in the OVI colour.

One possible approach to the OVI colour change is to check whether a sufficient light difference of the dominant colour is captured. Since the colour of the OVI feature depends on current lighting conditions, we can hardly compare the absolute values of the colours but rather look at the relative changes in the individual components. As discussed in section II-C2, the V component of the HSV colour model mostly follows the OVI colour change. Therefore, it is enough to check only the change in brightness, i.e., the V value component of the OVI dominant colour.

The inputs to the method are OVI dominant colours from image cuts detected in the detection part. From all input colours, the minimum and maximum value of component V is found. The difference between the minimum and maximum value of V represents the overall change in the brightness of the OVI feature in the video. If the change in brightness is big enough, the OVI colour and the ID card position change in the video. And as a result, the ID card is not marked as a counterfeit.

## III. Results

In the following section are summarized results of discussed methods and the proposed OVI feature verification procedure.

### A. Dataset

We created a dataset that consists of videos capturing real or counterfeit ID cards. The part of the dataset with real ID cards contains 92 videos of different lengths, taken in slightly different lighting conditions and by four different mobile phones with camera flash as a primary light source. Each video captures one of four real ID cards, with different types of OVI symbols. The background of the ID cards is either plain, textured or a complex scene. The position of the ID card to the mobile phone is achieved by moving the phone or the ID card in the user's hand. We put in the effort to imitate real conditions where the verification process could be used.

To test the proposed verification procedure, we created the second part of the dataset with fake ID cards. There are different forms of the falsification of ID cards. We recorded 71 videos of ID cards printed on classic office paper or photo paper. The videos are created similarly to the videos in the real dataset part, but counterfeit ID cards are used instead of real ID cards. Information about the dataset is summarized in Table I.

TABLE I. DATASET SUMMARY

| | Count |
|---|---|
| Real ID cards | 92 videos |
| Counterfeit ID cards | 71 videos |

### B. Detection of ID card

Detection of ID cards by using SIFT algorithm was tested on our dataset videos. In Table II, results show the method's sensitivity to correctly finding ID cards in video frames. The algorithm is more successful on real ID cards, and its overall success rate is 91.24% on the whole dataset. The ID card is not detected if the algorithm does not find a sufficient number of keypoints. The threshold is as high enough to ensure that the ID card is not incorrectly marked as detected.

TABLE II. DETECTION OF ID CARD USING SIFT ALGORITHM

| | real | counterfeit | all IDs |
|---|---|---|---|
| detected | 5747 | 3341 | 9088 |
| not detected | 388 | 484 | 872 |
| success rate | 93,68% | 87,35% | 91,24% |

### C. Detection of OVI security feature

Results of the detection of the OVI feature are discussed separately for the detection using Template Matching and SIFT and for the detection using Template Matching and SIFT extended with glitter verification. Only the solution with glitter verification is incorporated into the proposed OVI verification procedure.

The methods were tested on normalized ID cards obtained from videos from our dataset. In the results, incorrect indicates the image cut was made at the wrong position.

*1) Detection using Template Matching and SIFT:* Our method for the detection of the OVI security feature, which is the combination of Template matching and SIFT algorithm, has the results summarized in Table III. Detection is again less successful on counterfeit IDs, and its overall success rate is 91.48%.

TABLE III. DETECTION OF OVI SECURITY FEATURE WITHOUT GLITTERING

| | real | counterfeit | all IDs |
|---|---|---|---|
| correct | 5428 | 2886 | 8314 |
| incorrect | 319 | 455 | 774 |
| success rate | 94,45% | 86,38% | 91,48% |

*2) Detection using Template Matching and SIFT with glitter verification:* Glitter verification was tested on OVI image cuts from videos from our dataset. The comparison of OVI edge scores of real and counterfeit ID cards is in Fig. 11. In the histogram, both of them have two peaks with similar score values. Therefore, the edge score can not be included in the detection of the counterfeit.

On the other hand, the histogram in Fig. 12 properly separates correctly and incorrectly detected OVI image cuts, with the edge score threshold being approximately 100 000. Thus, the edge score can be used to exclude wrong OVI image cuts.

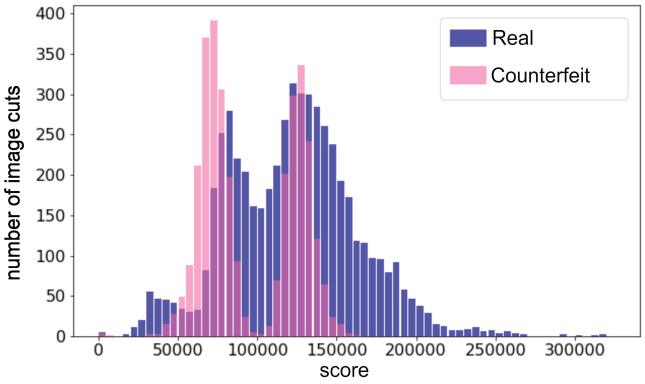



Fig. 11. OVI edge scores of real and counterfeit ID cards

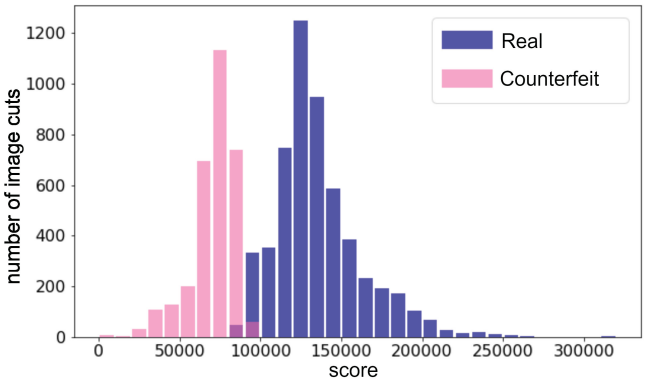



Fig. 12. Edge scores of correct and incorrect OVI cuts

Detection of the OVI feature using Template matching and SIFT supplemented with glitter verification has the results summed up in Table IV. The success rate is above 99% for both real and counterfeit ID cards. It indicates that almost no incorrect OVI image cut gets to the following analysis steps. However, many images were excluded, despite being correctly detected. Approximately 75% of all excluded frames were correct OVI image cuts.

TABLE IV. DETECTION OF OVI SECURITY FEATURE WITH GLITTERING

| | real | counterfeit | all IDs |
|---|---|---|---|
| correct | 5744 | 3329 | 9073 |
| incorrect | 3 | 12 | 15 |
| success rate | 99,95% | 99,64% | 99,83% |

For 37 counterfeit test videos from the dataset, no OVI image cut was detected in any single frame. Hence, if the detector is not able to find any ID card or OVI feature in the video, the detector will reveal counterfeit ID cards, even before OVI visual verification.

Fig. 13a shows an example of an incorrect OVI image cut that passed all detection steps. Several factors influenced the false detection, specifically the image is remarkably dark, and the OVI feature is slightly deformed. Deviation and distortion of OVI can occur, e.g., if the ID card is captured at an almost

(a) High-Incorrect (b) Low-Incorrect (c) Low-Correct

Fig. 13. Edge Score - Cut Correctness

perpendicular angle to the camera or if the counterfeit ID card is not straight but slightly bent.

In Fig. 13b, there is an incorrect OVI image with a low edge score and thus is correctly excluded from further analysis. Fig. 13c demonstrates the opposite situation when a correct OVI cut is made but evaluated with a low score. However, the image is obviously of low quality and too bright. This type of error commonly occurs in low-quality, blurred or overexposed images when the OVI feature does not have the expected visual properties at all.

### *D. Visual verification of captured change in OVI colour*

The change of brightness in the dominant colour was analysed on videos from our dataset. Fig. 14 is a histogram with overall changes in brightness captured in videos. The change in brightness captured in videos with counterfeit ID cards is noticeably smaller than with real IDs. Furthermore, we found that in real ID card videos with a low brightness change, the ID card was not moved and rotated enough to capture the sufficient OVI colour change.

Based on the histogram, we can specify the threshold value of the brightness change, that is the minimum required difference between the lowest and the highest value of the V component in the video. Thus it detects the counterfeit ID card according to the overall brightness change in the video.

### *E. Proposed OVI feature verification procedure*

In the first step, ID cards are detected and normalized in input video frames. Then OVI image cuts are found, and glittering is verified. All detected OVI image cuts step into the visual verification part, which is yet the verification of captured change in OVI brightness discussed in section III-D.

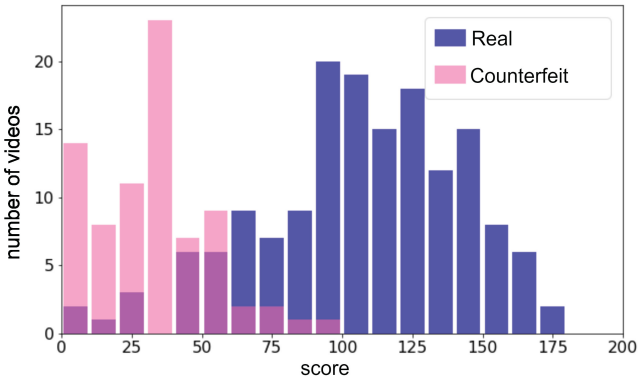



Fig. 14. The change in brightness in videos

And thus, the results of the brightness change check are equal to the results of the proposed OVI security feature verification procedure.

The procedure was tested on videos from our dataset, and results are summarized in the following Tables V and VI. In a confusion matrix is a higher number of false positives. Therefore, the proposed verification process is more sensitive than precise, and the accuracy is 82.82%.

TABLE V. CONFUSION MATRIX OF THE FULL VERIFICATION

| | predicted real | predicted counterfeit |
|---|---|---|
| actual real | 66 | 26 |
| actual counterfeit | 2 | 69 |

TABLE VI. RESULTS OF THE FULL VERIFICATION

| | |
|---|---|
| Accuracy | 82,82% |
| Sensitivity | 97,18% |
| Precision | 72.63% |

## IV. CONCLUSION

This paper provides the analysis of the OVI security feature and proposes the OVI verification procedure divided into several steps. We can detect an ID card in video frames with a sensitivity of 91.24%. The sensitivity of OVI detection in ID card images is 99.83%. The proposed OVI verification procedure can detect a counterfeit ID card on video based on the OVI feature analysis with 82.82% accuracy.

The proposed OVI feature verification procedure has some limitations and can be improved in various ways; however, a larger volume of data is needed. Obtaining high-quality data is problematic because of personal data protection, but necessary for a more complex solution.

Firstly, the verification of the OVI colour with respect to the ID card position must be added to the verification procedure. The proposed procedure omits this verification step but it is recommended to be added to get a reliable and secure system. A transformation matrix from the ID card normalization step represents the information about the OVI position in the image. The matrix directly or its modification can be included in the verification method of this visual property.

A more sophisticated solution could omit the requirement for the camera flash as the primary light source, and therefore, the position of the light source can differ from the camera position. A model without this condition could consider the changing position of the light source separately from the camera sensor.

In the discussed methods, the HSV chromatic component H of the dominant colour is neglected due to the influence of lighting conditions. A more complex model could also include this colour component. One option is to create a separate model for the H component. The second alternative is a more complex model, which includes all three HSV components. Another solution may use a more complex representation of

colour, e.g., histograms, heatmaps of colour components, or the entire image of the OVI feature.

A more complex model could also consider the time of the frames and their order. Such a model could understand the context of the frame within the sequence while working with time series over 2-dimensional data. The current solution considers the ID card transformation, not the order of the frames. Another modification could work with representative frames, not the whole video sequence. Representatives may be chosen in some sophisticated way, e.g., by clustering the frames.

In conclusion, the proposed OVI feature verification procedure is the solution that arose from the first analysis of this problem. The proposed verification procedure has several limitations, and some partial problems still need to be solved. Discussed methods can be further researched and improved or become a starting point for more sophisticated methods. Additionally, some of the methods can be reused in the verification process of other security features with similar visual characteristics or might be extended to other document types or completely different objects with similar security features, e.g., banknotes. Based on our results, we can conclude that the digital verification of security features has potential for future research.

## ACKNOWLEDGEMENT

This research was supported by the Ministry of Education, Science, Research and Sport of the Slovak Republic under the contract No. VEGA 1/0369/22. This publication has been produced with the support of the Integrated Infrastructure Operational Program for the project "Integrated strategy in the development of personalized medicine of selected malignant tumor diseases and its impact on life quality", ITMS code: 313011V446, co-financed by the European Regional Development Fund.

## REFERENCES

[1] A. Hartl, J. Grubert, D. Schmalstieg, and G. Reitmayr, "Mobile interactive hologram verification," in *2013 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE, 2013, pp. 75–82.

[2] D. Soukup and R. Huber-Mörk, "Mobile hologram verification with deep learning," *IPSJ Transactions on Computer Vision and Applications*, vol. 9, no. 1, pp. 1–6, 2017.

[3] B. Ay, "Open-set learning-based hologram verification system using generative adversarial networks," *IEEE Access*, vol. 10, pp. 25 114–25 124, 2022.

[4] G. A. R. Sanchez, "A computer vision-based banknote recognition system for the blind with an accuracy of 98% on smartphone videos," *Journal of The Korea Society of Computer and Information*, vol. 24, no. 6, pp. 67–72, 2019.

[5] MISR, "Ministry of Interior of the Slovak Republic, Security features of indentity cards released since 1.7.2008 (in Slovak)," 2008. [Online]. Available: https://www.minv.sk/?vzory-dokladov

[6] ——, "Ministry of Interior of the Slovak Republic, Security features of indentity cards released since 30.11.2013 (in Slovak)," 2013. [Online]. Available: https://www.minv.sk/?vzory-dokladov

[7] ——, "Ministry of Interior of the Slovak Republic, Security features of indentity cards released since 1.3.2015 (in Slovak)," 2015. [Online]. Available: https://www.minv.sk/?vzory-dokladov

[8] Council of the EU, "General Secretariat of the Council of the European Union, PRADO - Public Register of Authentic identity and travel Documents Online," 2022. [Online]. Available: https://www.consilium.europa.eu/prado/sk/prado-glossary/prado-glossary.pdf

[9] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, no. 2, pp. 91–110, 2004.

[10] OpenCV, *OpenCV metrics for Template Matching*, 2021. [Online]. Available: https://docs.opencv.org/4.5.5/df/dfb/group__imgproc__object.html

[11] T. Gevers, A. Gijsenij, J. Van de Weijer, and J.-M. Geusebroek, *Color in computer vision: fundamentals and applications*. John Wiley & Sons, 2012, vol. 23.

[12] D. Taylor, T. Hallett, P. Lowe, and P. Sanders, *Digital photography complete course*. DK Publishing, 2015.