

EXPRESS PAPER

Open Access



Mobile hologram verification with deep learning

Daniel Soukup* and Reinhold Huber-Mörk

Abstract

Holograms are security features applied to security documents like banknotes, passports, and ID cards in order to protect them from counterfeiting. Checking the authenticity of holograms is an important but difficult task, as holograms comprise different appearances for varying observation and/or illumination directions. Multi-view and photometric image acquisition and analysis procedures have been proposed to capture that variable appearance. We have developed a portable ring-light illumination module used to acquire photometric image stacks of holograms with mobile devices. By the application of Convolutional Neural Networks (CNN), we developed a vector representation that captures the essential appearance properties of hologram types in only a few values extracted from the photometric hologram stack. We present results based on Euro banknote holograms of genuine and counterfeited Euro banknotes. When compared to a model-based hologram descriptor, we show that our new learned CNN representation enables hologram authentication on the basis of our mobile acquisition method more reliably.

Keywords: Mobile security inspection, Photometric hologram verification, Deep learning

1 Introduction

Holograms or Diffractive Optically Variable Image Devices (DOVID) change their appearances when viewed and/or illuminated under different angles (Fig. 1) and are a means to protect security documents (e.g., banknotes, passports) from counterfeiting. Checking their authenticity is an important, but still, challenging task. In practice, the holograms' grating structures are analyzed with microscopes or sparse point-wise projection and recording of the diffraction patterns [1]. For example, the *Universal Hologram Scanner* (UHS) [2] is a well known tool for hologram verification actually used in forensic analyses, where the holograms' diffraction patterns are analyzed at discrete steps over the hologram area.

A guided multi-view approach for hologram acquisition for mobile devices in order to capture hologram appearance variations was proposed recently [3], which further allowed for hologram detection and tracking [4]. A machine vision system combining multi-view and photometric approaches by acquiring holograms for different illumination angles with a light-field camera was proposed [5] in a recent publication. As illumination unit, a

photometric light-dome of 30 cm in diameter comprising 32 LEDs was presented. Despite the availability of multi-view information, the authors could only make use of the photometric variation in the data. By modeling the photometric reflectance properties, they developed a low-dimensional hologram representation, in which the essentials of holograms' appearances are compressed into only a few hundred vector entries. The properties of that so called *DOVID descriptor* were reported recently [6, 7].

We developed a portable ring-light module that can be mounted to a mobile device to make photometric acquisitions (Fig. 2), similar to the aforementioned illumination dome. Moreover, we additionally developed a new vector representation for holograms by means of deep learning a CNN from the holograms' photometric image stacks. While for our data, the modeled DOVID descriptor was tedious to parameterize and parameterization could only be accomplished with the aid of counterfeited holograms at hand, our new learned hologram representation is solely learned from genuine holograms. Nonetheless, the description is robust enough, to be able to reliably distinguish fake holograms from genuine holograms of the intended type.

The rest of the paper is structured as follows. In Section 2, we describe the acquisition system comprising

*Correspondence: daniel.soukup@ait.ac.at
AIT Austrian Institute of Technology GmbH, Donau-City-Straße 1, 1220 Vienna, Austria

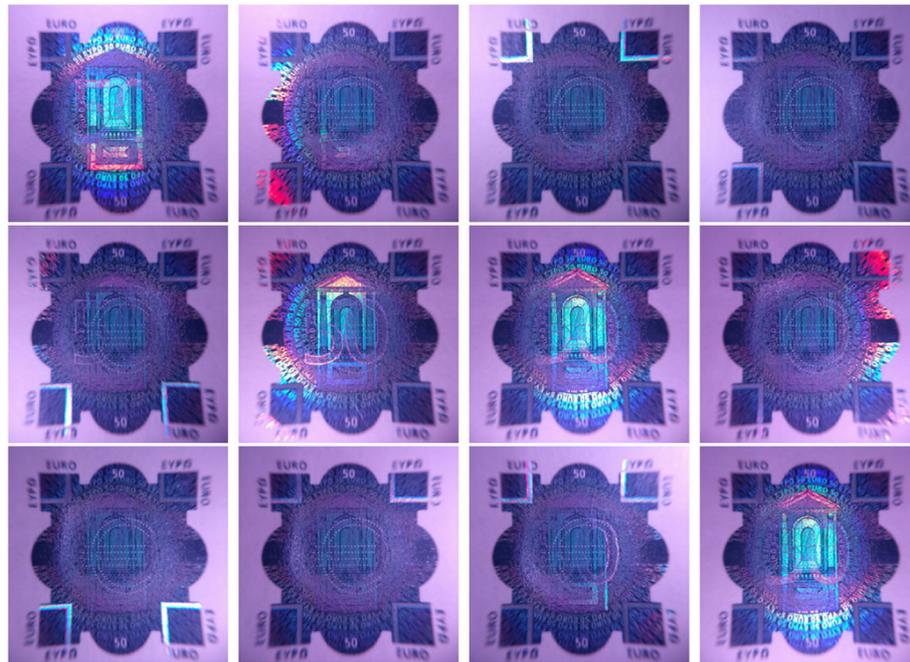


Fig. 1 Appearances of a Euro 50 hologram illuminated from 12 different directions

the portable ring-light module mounted to a Nexus P6 mobile device. The generation of the new hologram vector representation is outlined in Section 3. An experimental evaluation and comparison with a model-based representation based on the data sample described in

Section 4 is given in Section 5, followed by the summary and conclusions in Section 6.

2 Mobile photometric hologram acquisition

The appearances of holograms shall be captured in a photometric image stack, which is a set of images taken from an object, e.g., a hologram, under different illumination directions. While similar work [6] used a rigid, rather bulky setup of a camera and a large illumination device, we intend to do acquisitions with a mobile device. In particular, for this study, we used a Nexus 6P from Google comprising a 12.3 MP camera. For that device, we developed an illumination module (Fig. 3) comprising a 3D printed retainer, a LED strip of 24 individually operable LEDs (WS2812b) mounted to the inner walls of the cylindrical dome (Fig. 4), and corresponding controls so that the LED module was controllable via the mobile device.

Due to the small diameter of the LED ring, acquisitions had to be done in very close range in order to achieve sufficiently large illumination angles to make the variability of the holograms visible. Thus, it was necessary to additionally mount a macro and wide-angle lens (Mantona 18672 objective set) to the NEXUS P6 to make the field of view wide enough.

The coordination of acquisition and illumination was controlled by a software, i.e., control of focus, exposure time, switching of illuminating LEDs, and actual acquisition. A single hologram is acquired 24 times, once for each illuminating LED, whereby the observation position is held constant. We call the resulting photometric set of



Fig. 2 Mobile photometric hologram acquisition setup

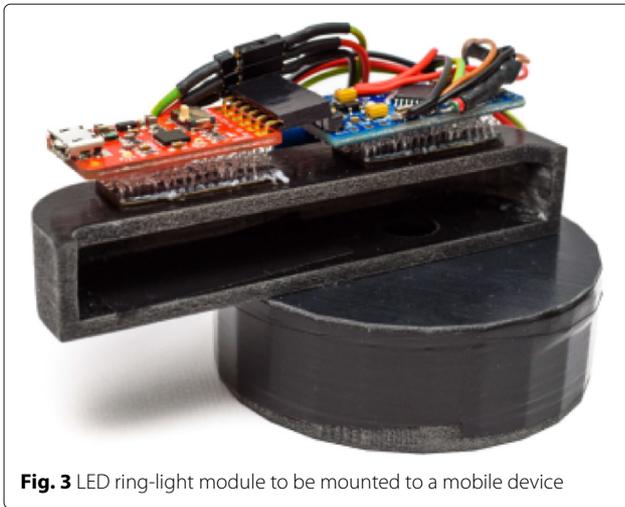


Fig. 3 LED ring-light module to be mounted to a mobile device

24 RGB images the *Photometric Hologram Stack* (PHS). When stacked along the color channel dimension, the PHS is a 3D array with $3 \times 24 = 72$ color channels.

3 Compressed hologram representation by deep learning

Given a PHS of a hologram, the goal is to generate a compressed representation of the variations that allows for easily comparing different holograms. We will compare our approach to the so called DOVID descriptor [6] which extracts properties of the Bidirectional Reflectance Distribution Function (BRDF) for each hologram position out of (in their case) the 32 available color values for each position. The final descriptor was constructed as a histogram vector of these properties over all hologram positions. The optimal parameterization of property thresholds, masking, and histogram bins has to be assessed by trial and error with the objective that fake holograms distinctly differ from the corresponding intended genuine hologram types. That means that a sufficient sample of fakes must be at hand during training, which is often difficult to achieve.

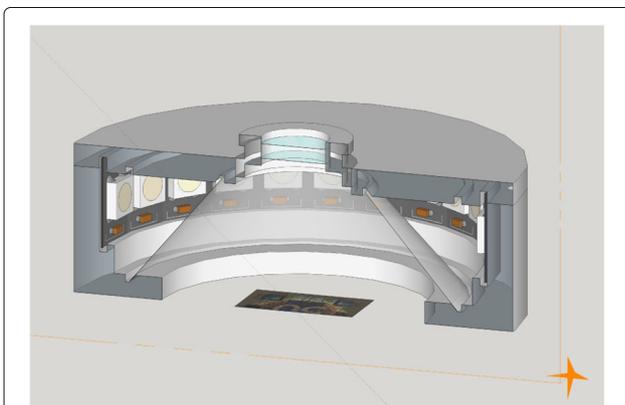


Fig. 4 Illustration of a cross-section of the cylindrical LED ring light-dome

Thus, an alternative method of generating reliable hologram representations is required, which

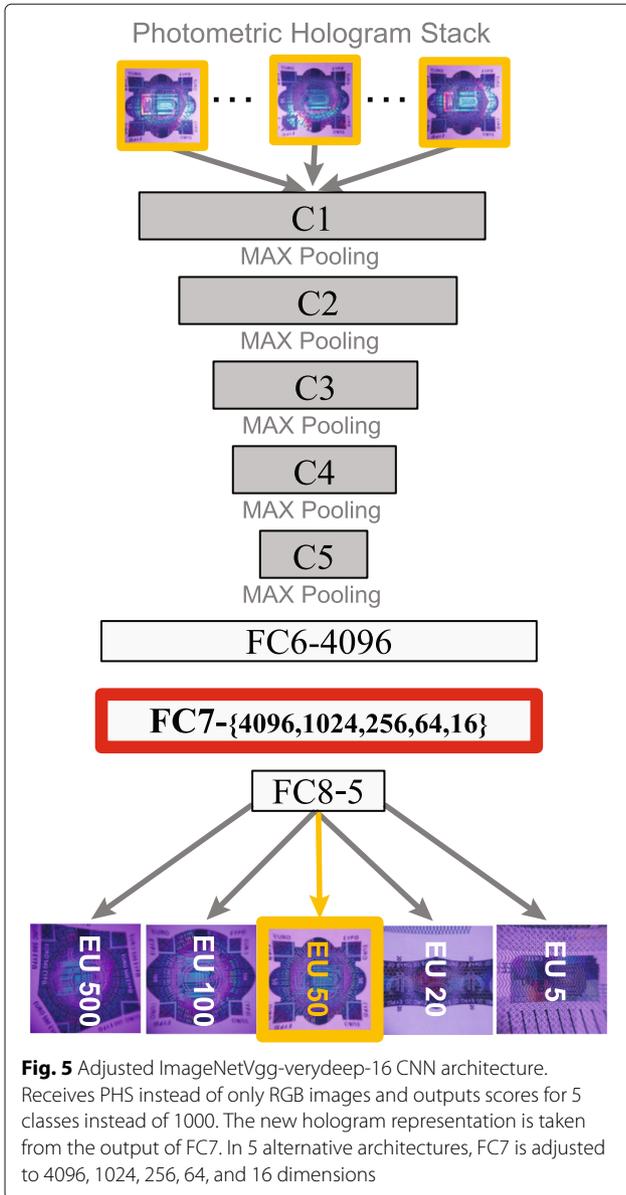
- (1) learns hologram types' target appearances only from genuine samples,
- (2) learns from the PHS directly without much image pre-processing, and
- (3) reflects measurable deviations from genuine references for newly presented fakes.

Motivated by the great success of deep learning in various computer vision tasks over the last years, we employed deep learning a Convolutional Neural Net (CNN) for this task. The training objective is to *classify PHS stacks of genuine hologram types* (in our case Euro banknote holograms, i.e., EU5, EU20, EU50, EU100, and EU500). We use the vector output of a high-level layer of the trained CNN as the new hologram representation vector. Thereby, on the basis of a vector metric, the representation of a new hologram is compared with hologram representations of reference holograms which are known to be genuine.

Due to our very small sample of holograms, we were forced to make use of transfer learning. Yosinski et al. [8] showed that CNN features learned in one task can be transferred to another task. Azizpour et al. [9] presented a detailed study on relevant factors for transfer learning. Especially, when there is only a small sample set available in the second task, a CNN pre-trained on the first task as initial setting for training the second task showed to be preferable to random initializing the CNN. This is called *fine-tuning* the CNN on the second task. Fine-tuning meanwhile is commonly used, often by means of CNNs trained on ImageNet, as these nets have been trained extensively on very large data sets. Similarly to Wang et al. [10], we initialized our CNNs with the fully pre-trained CNN *ImageNetVgg-verydeep-16-4096* [11] trained by the Visual Geometry Group Oxford on the ILSVRC-2012 data set [12]. This architecture receives $224 \times 224 \times 3$ color images as input. In the convolutional part, those are processed through five convolutional blocks C1, C2, C3, C4, and C5 with 2, 2, 3, 3, and 3 convolutional layers, respectively, followed by 3 fully connected layers FC6, FC7, and FC8. Each convolutional block is completed by a max-pooling layer (Fig. 5).

To allow for the input of PHS, which in our case are image arrays with 72 "color channels," we copied the first convolutional layer weights 24 times. In the original setup, FC8 provides a 1000-vector representing probability scores of the 1000 object classes in the ImageNet2012 challenge. According to merely 5 hologram types to be classified in our task, we reduced FC8's output to a 5-vector.

As the new hologram representation, the highest-level CNN representation is used, which is the output



of FC7. Originally, FC7 is 4096-dimensional, which is far higher dimensional than the aforementioned model-based DOVID descriptor which is 150-dimensional in our experiments. Thus, we conducted experiments with alternative architectures, where FC7 outputs 4096-, 1024-, 256-, 64-, and 16-dimensional representations. Those five different architectures shall be referred to as *FC7-4096*, *FC7-1024*, *FC7-256*, *FC7-64*, and *FC7-16*.

4 Sample holograms

By courtesy of the OeNB¹, we had an access to samples of genuine Euro banknotes of the five denominations EU5, EU20, EU50, EU100, and EU500. Each genuine denomination contains a different type of hologram. For each of the five types, we acquired ten examples of genuine

holograms. Additionally, ten examples of genuine but severely creased EU5 banknotes were available, which can be used to determine if the developed CNN hologram representation shows a similar structure for creased and uncreased holograms. This would be an important evidence of robustness to crease, as crease is a very natural source of variation of banknotes. While the EU5 sample only contains genuine holograms, for the other types, a number of counterfeited holograms were acquired, i.e., 16 examples for EU20, 23 examples for EU50, 14 examples for EU100, and 9 examples for EU500.

By means of our acquisition setup from Section 2, for each hologram, 24 RGB images were acquired, one for each of the ring-light device's LEDs. Hologram areas were cutout from the images and sampled so that each image is filled predominantly by the hologram and that it comprises a 224×224 pixel raster, which is the spatial input size for the CNN. Those 24 $224 \times 224 \times 3$ images were stacked along the color channel into the $224 \times 224 \times 72$ dimensional PHS.

5 Experimental results

The five CNN architectures *FC7-4096*, *FC7-1024*, *FC7-256*, *FC7-64*, and *FC7-16* were setup on a pre-trained ImageNetVgg-verydeep-16 CNN provided by the Visual Geometry Group Oxford as described in Section 3. Each CNN was fine-tuned for further 30 epochs with the fixed learning rate $\alpha = 1e - 5$ and the objective to classify genuine Euro holograms of the types EU5, EU20, EU50, EU100, and EU500 (see Section 4). For each hologram type, seven genuine samples were used for training and three for validation. Additionally, data augmentation was applied, where each training sample was augmented by two randomly shifted (≤ 15 pxl) and two randomly rotated ($\leq 8^\circ$) versions in each epoch. Well before epoch 30, each of the CNNs could classify genuine holograms perfectly.

After fine-tuning, each hologram PHS was processed through each of the CNNs and the corresponding hologram representation vectors received from the FC7 layers. In parallel, for each hologram, the histogram-based, modeled DOVID descriptor was generated. Required parameters were set by trial and error search using also the fakes with the objective that fake representations should distinctly differ from genuine ones. The final solution led to a 150-dimensional histogram representation to which we refer as *Hist-150*.

Thus, for a fixed representation type $R \in \{FC7-4096, \dots, FC7-16, Hist-150\}$ of dimension $m \in \{4096, 1024, 256, 64, 16, 150\}$ and a hologram type $H \in \{EU5, EU20, EU50, EU100, EU500\}$, let

$$G_H^R = \{g_i \in \mathbb{R}^m\}, \quad F_H^R = \{f_i \in \mathbb{R}^m\} \quad (1)$$

be the sets of representations of the genuine holograms G_H^R and faked holograms F_H^R . Note, F_{EU5}^R contains the set of indeed genuine, but severely creased, EU5 banknotes and no fakes.

In order to mutually compare hologram representations, we use the *cosine distance* as measure of dissimilarity of any two hologram representation vectors $p \in \mathbb{R}^m$ and $q \in \mathbb{R}^m$:

$$d_{\cos}(p, q) = 1 - \frac{\langle p, q \rangle}{\|p\|_2 \cdot \|q\|_2}. \quad (2)$$

For a hologram fake to be detectable as counterfeit, its nearest neighbor distance to the cluster of genuine hologram representations of the corresponding hologram type must be significantly larger than the maximal intra-cluster distance of mutual distances between the genuine holograms, i.e.,

$$\forall f \in F_H^R : \min \{d_{\cos}(f, g_i) | g_i \in G_H^R\} \gg \max \{d_{\cos}(g_i, g_j) | g_i, g_j \in G_H^R, i \neq j\}. \quad (3)$$

In this manner, we define a *fake separation factor* s_H^R , which indicates how well all available fake holograms are distinguishable from the genuine holograms of the hologram type intended to be faked, i.e.,

$$s_H^R := \frac{\max \{d_{\cos}(g_i, g_j) | g_i, g_j \in G_H^R, i \neq j\}}{\min \{d_{\cos}(f, g_j) | f \in F_H^R, g_j \in G_H^R\}}. \quad (4)$$

In s_H^R , the maximum intra-genuine-cluster distance is set in relation to the minimum fake-to-genuine-cluster distance. If all the fakes $f \in F_H^R$ are well distinguishable from the corresponding genuine holograms in G_H^R , then $s_H^R \ll 1$. If $s_H^R \geq 1$, then at least one $f \in F_H^R$ at least touches the genuine hologram cluster G_H^R indicating that F_H^R cannot reliably be distinguished from the genuine holograms.

In Table 1, the fake separation factors s_H^R are listed for all hologram types and representation types. For *CNN representations*, results show the following:

Table 1 Fake separation factor s_H^R for all hologram types and all types of hologram representation vectors

Type	EU5	EU20	EU50	EU100	EU500
FC7-4096	1.33	0.3	0.24	0.29	0.11
FC7-1024	1.38	0.22	0.2	0.23	0.1
FC7-256	1.01	0.22	0.16	0.13	0.07
FC7-64	2.01	0.33	0.08	0.06	0.06
FC7-16	3.2	0.18	0.03	0.06	0.06
Hist-150	0.84	0.09	1.04	0.18	0.24

Note for EU5 no fakes are available, here we measured the separation between flat and creased genuine holograms

- That fakes are reliably distinguishable from genuine holograms ($s_H^{\text{FC7-*}} \ll 1$ for $H \in \{\text{EU20, EU50, EU100, EU500}\}$),
- Robustness to crease ($s_{EU5}^{\text{FC7-*}} > 1$ shows that creased and uncreased holograms are indistinguishable)², and
- High compression rate (representations are robust even for $m = 16$).

The *DOVID descriptor* on the other hand does not have that robustness to crease as $s_{EU5}^{\text{Hist-150}} = 0.84 < 1$ indicates a gap between creased and uncreased hologram clusters. $s_{EU50}^{\text{Hist-150}} = 1.04 > 1$ further shows, that also fake detection could not be accomplished reliably.

6 Conclusion

We presented a mobile setup for photometric hologram acquisition by means of an especially constructed portable ring-light module mountable to a mobile device. In order to evaluate the obtained photometric hologram image stacks, we developed a new hologram representation for capturing and compressing the essential appearance properties of holograms with methods of deep learning. We compared its capability of fake detection on Euro banknote holograms with that of an already existing histogram-based photometric hologram descriptor. While our new learned representation can be easily computed only by the use of a genuine hologram sample, the already existing descriptor can only be parameterized by using a sample of fakes as well. Nevertheless, our hologram representation is more robust to natural hologram appearance variations and could more reliably detect fake holograms, despite those which have never been used in the training stage.

Endnotes

¹ National Bank of Austria (OeNB), Test Center, Vienna

² In a more detailed cluster analysis, we also verified that the CNN representations of the creased EU5 holograms are actually embedded in the cluster of genuine uncreased EU5 representations.

Acknowledgements

We acknowledge the National Bank of Austria (OeNB), Test Center Vienna, for providing us with genuine and faked hologram samples.

Funding

Not applicable.

Availability of data and materials

Data cannot be shared, as they contain security features of EURO banknotes and are not allowed to be published.

Authors' contributions

In all the stages of the work, both authors have similar contributions. Both authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Consent for publication

Not applicable.

Ethics approval and consent to participate

Not applicable.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 17 February 2017 Accepted: 9 March 2017

Published online: 24 March 2017

References

1. van Renesse RL (2005) Optical document security. 3rd edn. Artech House, Boston London
2. van Renesse RL (2005) Testing the universal hologram scanner: a picture can speak a thousand words. *Keesing J Doc Identity* 12:7–10
3. Hartl A, Grubert J, Schmalstieg D, Reitmayr G (2013) Mobile interactive hologram verification. In: *Proc. Intl. Symp. on Mixed and Augmented Reality (ISMAR)*. IEEE, Adelaide. pp 75–82
4. Hartl A, Arth C, Schmalstieg D (2014) AR-based hologram detection on security documents using a mobile phone. In: *Proc. Intl. Symp. on Visual Computing (ISVC)*. Springer, Las Vegas. pp 335–346
5. Štolc S, Soukup D, Huber-Mörk R (2015) Invariant characterization of DOVID security features using a photometric descriptor. In: *Proc. IEEE Intl. Conf. on Image Processing (ICIP)*. IEEE, Quebec City
6. Soukup D, Štolc S, Huber-Mörk R (2015) Analysis of optically variable devices using a photometric light-field approach. In: *Proc. SPIE-IS&T Electronic Imaging – Media Watermarking, Security and Forensics*. SPIE-IS&T, San Francisco
7. Soukup D, Štolc S, Huber-Mörk R (2015) On optimal illumination for DOVID description using photometric stereo. In: *Proc. Advanced Concepts for Intelligent Vision Systems (ACIVS)*. Springer, Catania. pp 553–565
8. Yosinski J, Clune J, Bengio Y, Lipson H (2014) How transferable are features in deep neural networks?. *CoRR abs/1411.1792:14*
9. Azizpour H, Razavian AS, Sullivan J, Maki A, Carlsson S (2016) Factors of transferability for a generic convnet representation. *IEEE Trans Pattern Anal Mach Intell* 38(9):1790–1802
10. Wang T, Zhu J, Ebi H, Chandraker M, Efros AA, Ramamoorthi R (2016) A 4D light-field dataset and CNN architectures for material recognition. *CoRR abs/1608.06985:16*
11. Simonyan K, Zisserman A (2014) Very deep convolutional networks for large-scale image recognition. *CoRR abs/1409.1556:14*
12. Russakovsky O, Deng J, Su H, Krause J, Satheesh S, Ma S, Huang Z, Karpathy A, Khosla A, Bernstein M, Berg AC, Fei-Fei L (2015) ImageNet Large Scale Visual Recognition Challenge. *Intl J Comput Vision (IJCV)* 115(3):211–252

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com
