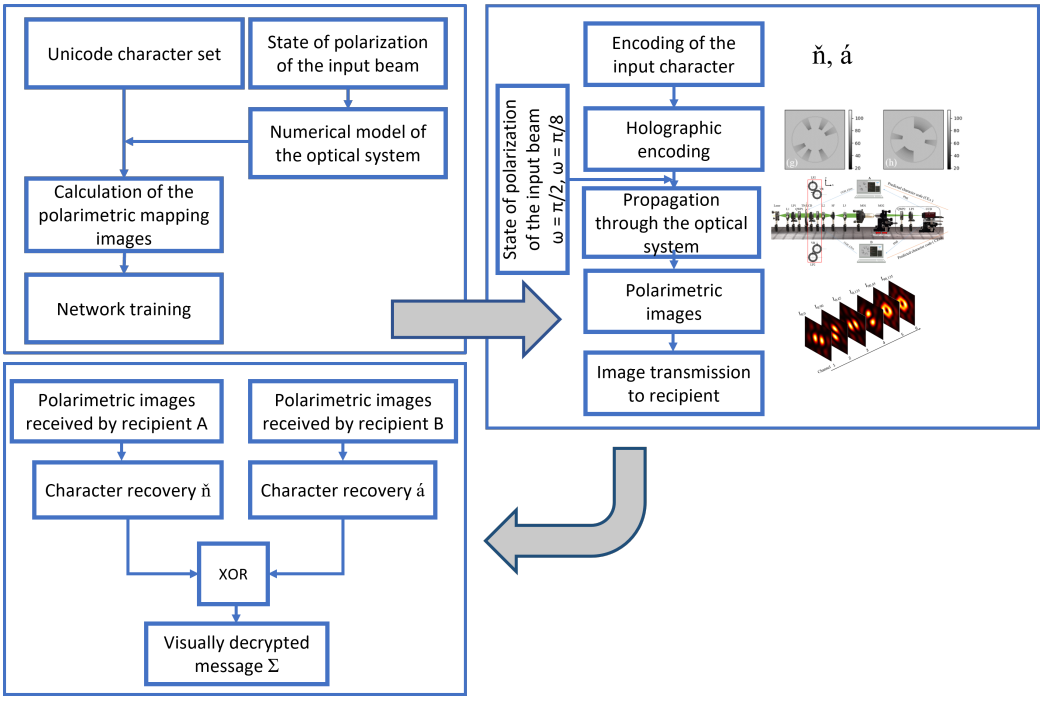
Graphical Abstract

Optical visual encryption using focused beams and convolutional neural networks

Kavan Ahmadi, Artur Carnicer[1]



[1]Corresponding author email: artur.carnicer@ub.edu

Highlights

Optical visual encryption using focused beams and convolutional neural networks

Kavan Ahmadi, Artur Carnicer[1]

- We present an optical implementation of the visual encryption method using focused fields and tunable spiral polarization.
- Our approach is able to deal with an arbitrary data-set of binary codes.
- The system is trained with a convolutional neural network using synthetic polarimetric focused field distributions.
- Our approach has been optically and numerically tested with a high success rate.

[1]Corresponding author email: artur.carnicer@ub.edu

Optical visual encryption using focused beams and convolutional neural networks

Kavan Ahmadi, Artur Carnicer[1]

Universitat de Barcelona (UB), Facultat de Física, Departament de Física Aplicada, Martí i Franquès 1, 08028 Barcelona (Spain)

Abstract

The target of this paper is to implement an optically-based visual encryption system able to work with a large set of optical codes. The optical setup comprises a holographic system designed to generate spirally-polarized highly focused fields and an imaging module able to perform polarimetric analysis. In a previous stage, the optical system is numerically simulated in order to produce synthetic polarimetric distributions that are used to train a convolutional neural network. Interestingly, the way the network is trained depends on the selected state of polarization. Then, secret codes are split in two XOR-connected ones that are optically processed. The corresponding experimental polarimetric distribution is obtained and transmitted to the corresponding recipients, that can recover the code by interrogating the neural network. Finally, combining the two pieces of information, the encrypted message can be decoded.

Keywords: Optical security, highly focused beams, neural networks

1. Introduction

In 1994 and 1995, Javidi and collaborators published the first papers on optical encryption [1, 2]. Since then, thousands of papers in this field have been published. As a matter of fact, according to both World of Science and Scopus, reference [2] has been cited more than 2000 times. The original double random phase encoding approach has been modified uncountable times to provide flexibility and improve security. These alternative techniques include

[1]Corresponding author email: artur.carnicer@ub.edu

the use of Fresnel diffraction [3, 4], fractional Fourier transforms [5, 6], logistic maps [7], phase-truncated transforms [8], holography [9, 10], interference [11, 12], wavelength multiplexing [13], ghost imaging [14], diffraction [15], gyrator transform [16], polarization [17, 18], or photon counting [19], just to cite some of them. Other papers analyzed flaws and weakness of optical encryption, mainly related with the properties of Fourier transforms [20–22]. Very recently, the generalized use of deep learning provides a new perspective for analyzing optical encryption problems (see, for instance, [23–30]). Note that it is practically impossible to cite all relevant work produced in the last years. For a more in-depth analysis, the interested reader might consider the following excellent reviews and references therein [31–36].

Furthermore, the study of electromagnetic beams with arbitrary amplitude and polarization is a very active research field [37]. Also, we have studied how polarimetric information, in combination with machine learning techniques, might be used in validation problems [38, 39]. One possible application of these techniques is in the field of optical security [40–43]. Despite these approaches uses of beams in the paraxial domain, the possibility of manipulating the longitudinal component of highly focused beams [44, 45] has also been considered [46, 47].

Secret sharing [48] and exclusive-OR visual encryption [49] are related security techniques that have also been ported to the optical domain. Interestingly, several papers considering optical problems using XOR-based encryption [50–53] or secret sharing related techniques [54–57] have been recently published. In this paper, we describe a system able to transmit text using the visual encryption paradigm. The characters of a string are sequentially processed, one at a time. The binary representation of every character of the string is split in two using the usual XOR approach [49]. Then, the two resulting characters are independently manipulated. Each character is holographically encoded and used as the input of an optical setup able to produce focused fields with tunable spiral polarization. Finally, the system records six polarimetric images that are transmitted to the recipient. The character can be recovered by interrogating a convolutional neural network (CNN) [58] that was trained in a previous stage; interestingly, the training set depends on the input polarization. Our approach was demonstrated using 10-bit Unicode characters, but the method can be used with an arbitrary binary-code data-set as well.

The paper is organized as follows: in section 2 we review basic concepts in focused fields. In section 3 we describe the steps and techniques required

to implement both the system and training the neural network. This involves (i) the character encoding procedure, (ii) the experimental setup, (iii) how the neural network is trained, and (iv) the results obtained. In section 4 we discuss the advantages and limitations of the proposed method and finally, we present our conclusion in section 5.

2. Review of basic concepts

The Richards-Wolf formula describes the behavior of a focused electromagnetic beam in the focal region of a high numerical aperture (NA) lens. This equation relates the transverse illuminating beam $\mathbf{E_0} = (E_{0x}, E_{0y}, 0)$ and the focused field at the focal plane ($z = 0$), $\mathbf{E}(r, \phi, z = 0)$ [59]

$$\mathbf{E}(r, \phi, 0) = A \int_0^{\theta_0} \int_0^{2\pi} \mathbf{E}_\infty(\theta, \varphi) \exp\left(ikr \sin\theta \cos(\phi - \varphi)\right) \sin\theta \, d\theta \, d\varphi \,, \quad (1)$$

where $\mathbf{r} = (r, \phi, z)$ are the coordinates at the focal area, A is a constant value, k is the wave-number, θ_M is the semi-aperture angle, and θ and φ are the coordinates at the Gaussian sphere of reference; NA is related to the semi-aperture angle θ_M by means of $\mathrm{NA} = \sin\theta_M$. $\mathbf{E}_\infty$ is the so-called vector angular spectrum:

$$\mathbf{E}_\infty = \sqrt{\cos\theta} \left((\mathbf{E_0} \cdot \mathbf{e}_1) \, \mathbf{e}_1 \, + \, \left(\mathbf{E_0} \cdot \mathbf{e}_2^i\right) \mathbf{e}_2 \right), \quad (2)$$

where $f_1 = \mathbf{E_0} \cdot \mathbf{e}_1$ and $f_2 = \mathbf{E_0} \cdot \mathbf{e}_2^i$ are the azimuthal and radial transverse components of the incident transverse field $\mathbf{E_0}$, respectively. The wave-front vector $\mathbf{s}$ reads

$$\mathbf{s} = (\sin\theta \cos\varphi, \sin\theta \sin\varphi, -\cos\theta) \,, \quad (3)$$

whereas vectors $\mathbf{e}_1$, $\mathbf{e}_2$ and $\mathbf{e}_2^i$ are described by:

$$\mathbf{e}_1(\varphi) = (-\sin\varphi, \cos\varphi, 0) \quad (4a)$$

$$\mathbf{e}_2^i(\varphi) = (\cos\varphi, \sin\varphi, 0) \quad (4b)$$

$$\mathbf{e}_2(\varphi, \theta) = (\cos\theta \cos\varphi, \cos\theta \sin\varphi, \sin\theta). \quad (4c)$$

Note that $\mathbf{e}_1$, $\mathbf{e}_2$ and $\mathbf{s}$ form a triad of mutually orthogonal right-handed system of unit vectors. Figure 1 summarizes the systems of coordinates used (a) at the entrance pupil, (b) at the Gaussian sphere of reference and (c) at the focal plane.

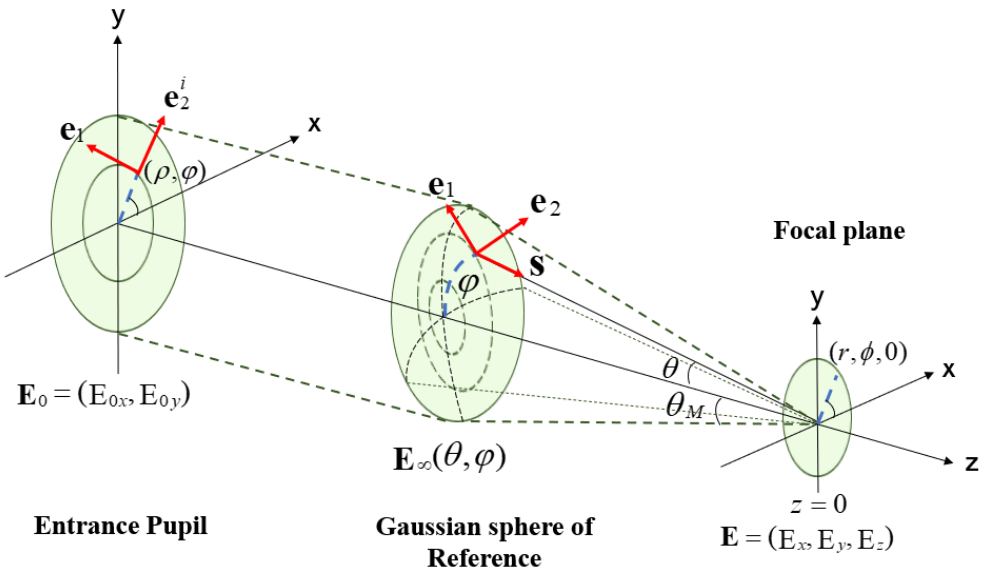


Figure 1: Coordinate system and geometrical magnitudes: (a) Entrance pupil, (b) Gaussian sphere of reference, and (c) focal plane.

Despite the input beam $\mathbf{E_0}$ is transverse to the optical axis, the focused beam $\mathbf{E}$ might display a non-negligible value in the longitudinal direction. Equation (1) can be written in terms of a λf-scaled Fourier transform (see [60])

$$\mathbf{E} = \mathrm{FT}_{\lambda f}\left[\frac{\mathbf{E}_\infty}{\cos\theta}\right], \tag{5}$$

where λ is the wavelength of the illuminating source and f is the focal length of the optical system. Interestingly, the components of the focused field $\mathbf{E}$ are not independent because the Gauss law $\nabla\mathbf{E}=0$ holds. In particular, the longitudinal component E_z in terms of the components of field $\mathbf{E_0}$ reads

$$E_Z = \mathrm{FT}_{\lambda f}\left[\frac{E_{\infty z}}{\cos\theta}\right] = \mathrm{FT}_{\lambda f}\left[\frac{\sin\theta}{\sqrt{\cos\theta}}\left(E_{0x}\cos\varphi + E_{0y}\sin\varphi\right)\right]. \tag{6}$$

If the beam is spirally polarized, components E_{0x} and E_{0y} are related by means of

$$E_{0x} = -E_{0y}\tan\left(\varphi+\omega\right), \tag{7}$$

being ω a parameter to be tuned. For instance, the beam is radially polarized when $\omega=\pi/2$.

In this paper, we decided to encode the information in such a way that the longitudinal component is explained as the Fourier transform of the information to be processed. Note that this is an arbitrary decision, and other alternatives might be considered as well. If the code to be processed is described by a circularly symmetric function $C(\varphi)$ (as explained in section 3.1) the $y-$component of the input beam $\mathbf{E_0}$ becomes

$$E_{0y} = C(\varphi)\frac{\sqrt{\cos\theta}}{\sin\theta}\frac{1}{-\cos\varphi\tan(\varphi+\omega)+\sin\varphi} \quad \text{with } \omega,\theta \neq 0\ , \qquad (8)$$

whereas the $x-$component E_{0x} is obtained by using Eq. (7). In such conditions, the longitudinal component of the focused beam becomes $E_z = \mathrm{FT}_{\lambda f}\left[C(\varphi)\right]$.

3. Methods

3.1. Encoding procedure

In 1979, Shamir published a short paper analyzing how to split a secret message S in N pieces of information with the following property: S should be fully recovered using K shares but not with $K-1$ [48]. In particular, if $N = K$, the method can be trivially implemented using the XOR logical operator. Note that for $N = K = 2$, secret sharing becomes the visual encryption scheme described in [49].

For demonstration purposes and without loss of generality, in this paper, we consider 10-bit messages shared by two parties using bit-wise XOR. These binary words can be graphically represented as Unicode characters ranging from 0 and 1023. This subset covers almost all characters used in western European languages, and also Greek and Coptic. For instance, randomly selected character code ň (U+0148) XOR-encoded with á (U+00E1) produces Σ (U+01A9); or using binary numbers, $0101001001 \oplus 0011100001 = 0110101001$, where symbol $\oplus$ stands for the bit-wise XOR operator. Note that some few codes do not correspond to actual characters (e.g., Null (U+0000), Bell (U+0007) or Escape (U+001B)), but could be encoded as well.

Binary information is arranged using an annulus of radii R_1 and R_0 ($R_1 > R_0$). The transmittance in the outer and inner parts of the annulus are zero, and values '1' or '0' are represented as transparent or opaque sectors respectively. In this way, $R_0 \neq 0$ (i.e., $\theta \neq 0$) and thus, no singularities are present in Eq. (8); R_1 is set equal to the radius of the illuminating beam at

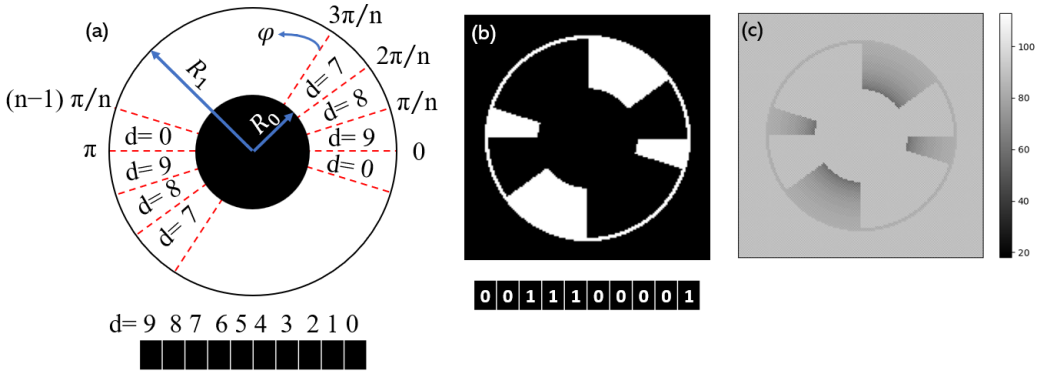


Figure 2: (a) Design of the encoding method. (b) Function $C(\varphi)$ encoding character (0011100001). (c) Corresponding computer generated hologram.

the entrance pupil of the microscope objective (Fig 1). In the present work, R_1=3.75 mm and R_0=1.8 mm. For a n-bit word, the annulus is split in $2n$ sectors to provide radial symmetry to the code. We name this procedure as circular encoder (CE) and is mathematically represented by $C(\varphi)$.

Figure 2(a) sketches the codification procedure of the circular encoder, and 2(b) displays $C(\varphi)$ corresponding to the character á (0011100001). In our design, instead of using just the binary pattern defined by $C(\varphi)$, the illumination beam $\mathbf{E_0}$ is modulated according to Eqs. (7 - 8). This real-valued distribution is introduced in the optical system using a computer generated hologram displayed on a liquid crystal device [61, 62], as described in the next section (see Fig. 2c).

Other authors have proposed similar approaches for encoding information to be used in an optical setup [63]. Moreover, a related, more complex arrangement was used by NASA to encode a message in the Mars Perseverance rover's parachute (see for instance [64]).

3.2. Experimental setup

The sketch of the optical system is shown in Fig. 3. The setup comprises two parts: a holographic system designed to generate spirally polarized focused fields and an imaging arrangement able to perform polarimetric analysis.

A pig-tailed laser with wavelength $\lambda = 520$ nm (Thorlabs LP520-SF15) illuminates a twisted nematic liquid crystal display (Holoeye HEO 0017,

1024×768 pixels and pixel pitch of 32 µm). Linear polarizer LP1 and quarter wave plate QWP1 set the modulation response of the display in phase-mostly configuration. The information to be processed is encoded using the Arrizon's double-pixel computer generated hologram technique [61]. Since Arrizon's holograms produce off-axis diffracted terms that should be filtered, lens L2 and L3 are set in a 4f configuration with a spatial filter (SF) placed in the back focal plane of L2. A more detailed explanation on how to produce custom focused beams with the help of computer generated holograms using liquid crystal displays can be found in [65–67].

In our approach, the beam is spirally polarized. The combined use of polarizer LP2 and vortex retarder VR (ThorLabs, WPV10L-532) enables us to produce this kind of beams. The particular polarization state, defined by w in Eq. (7), is obtained by modifying the relative angle of LP2 and VR respective axes. Finally, the beam is subsequently focused by means of microscope objective MO1 (Nikon Plan Fluorite N40X-PF with NA = 0.75). The microscope objective MO2 (Nikon, NA = 0.8) is placed on a movable stage driven by a motorized device (Newport LTA-HL) with repeatably of ±100 nm. This second objective is used to image the focused beam on the sensor plane of the CCD camera (Stingray with a 14-bit depth and a pixel pitch of 3.75 µm). Polarizer LP3 and quarter wave plate QWP2 are used to record six polarimetric images: $I_{0,0}$, $I_{0,45}$, $I_{0,90}$, $I_{0,135}$, $I_{90,45}$, and $I_{90,135}$. $I_{\alpha,\beta}$ stands for the recorded intensity when the linear polarizer is set at an angle β with respect to the x direction, and α is the phase delay introduced by QWP2.

3.3. Production of the training set

We produced two synthetic data-sets using a numerical procedure that simulates optical propagation across the system described in the previous section. Every data-set (namely A and B) uses a particular polarization state of the incident field $\mathbf{E_S}$: we selected $\omega = \pi/8$ and $\omega = \pi/2$ for data-sets A and B, respectively (see Eq. (7)). Note that training sets depend on the value of ω.

The complete collection of 1024 characters is used for training the system using a neural network. The proposed method will work with an arbitrary number of Unicode characters, but we decided to use a relatively small number of elements to be able to train the network quickly. For each character, we calculated the corresponding six polarimetric images that would be recorded at the sensor plane of the CCD. These six images are packaged in a single

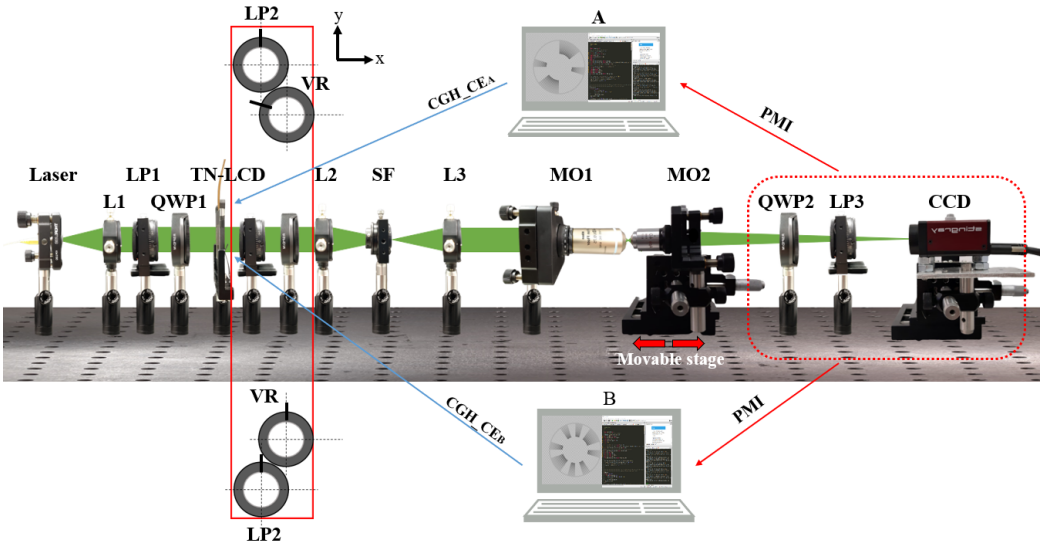


Figure 3: Optical setup: L1, L2, L3: lenses; LP1, LP2, LP3: linear polarizers; QWP1, QWP2: quarter wave plates; VR: Vortex retarder; SF: spatial filter; MO1, MO2: microscope objectives; CCD: camera. When VR is rotated, the polarization state of the beam is changed (see section 4). Figure adapted from [66] under a Creative Commons BY 4.0 license.

6-channel array; we refer to this multidimensional array as the Polarimetric Mapping Image (PMI). Figure 4 compares the calculated polarimetric images $I_{0,0}$, $I_{0,45}$, $I_{0,90}$, $I_{0,135}$, $I_{90,45}$, and $I_{90,135}$ with those obtained optically for character á using polarization cases A and B. Numerical results and optically recorded images display an excellent agreement. Since we are using non-uniform linear (spiral) polarization, images $I_{90,45}$, and $I_{90,135}$ should be identical. However, the two experimental distributions might be slightly different because $I_{90,45}$, and $I_{90,135}$ are recorded in different moments.

Data-sets A and B are generated according to the following steps:

1. The binary number that corresponds to the considered character was encoded using the procedure explained in section 3.1.
2. Then, the field $\mathbf{E_0}$ was generated taking into account the polarization state determined by ω (Eqs. (7-8)).
3. The transverse components of the focused field $\mathbf{E}$ (Eq. (1)) were calculated and used to generate the corresponding PMI.
4. To make the system resistant to noise and small changes in scale, related to possible experimental issues, we produced 8 different PMI for each

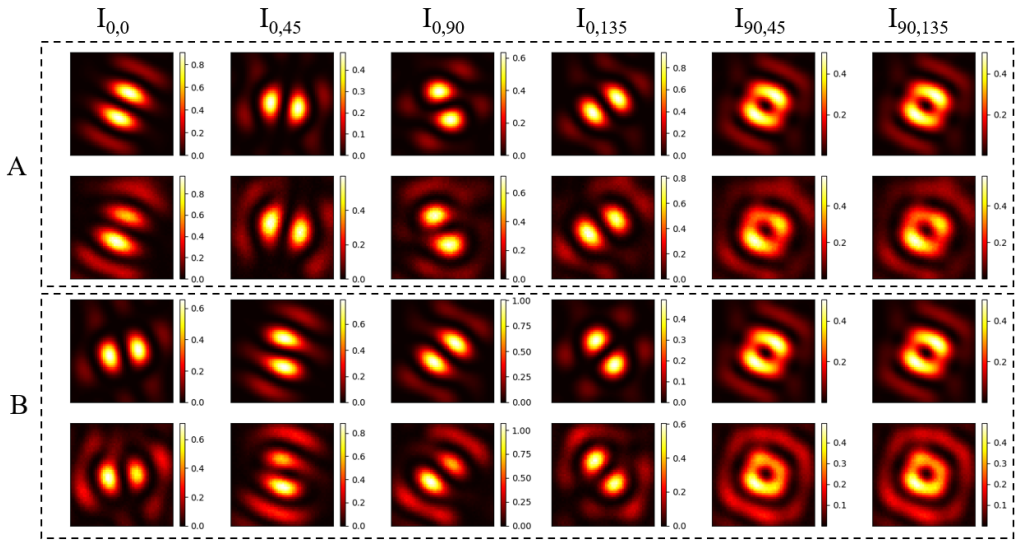


Figure 4: Results corresponding to character á (U+00E1): the first and second rows display numerically and optically obtained polarimetric images, respectively (case A). The third and fourth rows provide the same information, but for polarization case B.

character. These modified PMIs were generated from the original PMI (PMI_o), obtained in ideal conditions, as follows: (i) PMI_o was zoomed two times with scale factors 0.95 and 1.05, and (ii), PMI_o was corrupted with additive Gaussian noise with standard deviation σ equal to 0.05, 0.1, 0.15, 0.2 and 0.25 (we assume the arrays are normalized to 1). Accordingly, the data-set comprised 8192 PMIs (1024 characters x 8 PMIs per character). Figure 5 shows the first channels of the eight PMIs ($I_{0,0}$) corresponding to code ň (U+0148).

5. Finally, 6554 randomly selected PMIs were used for training whereas

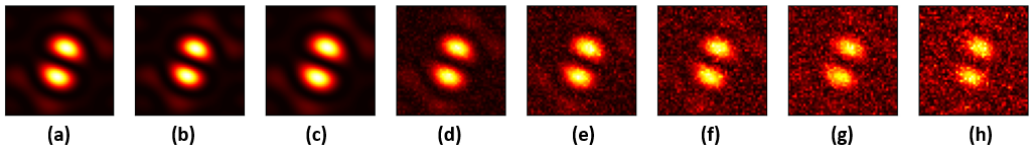


Figure 5: First channel ($I_{0,0}$) of the 8 PMIs for code ň (U+0148) calculated for polarization case A. (a) original PMI_o, (b) $I_{0,0}$ zoomed with scale factor = 0.95, (c) $I_{0,0}$ zoomed with scale factor = 1.05; $I_{0,0}$ corrupted with additive Gaussian noise: (d) $\sigma = 0.05$, (e) $\sigma = 0.1$, (f) $\sigma = 0.15$, (g) $\sigma = 0.2$, and (h) $\sigma = 0.25$.

the remaining 1638 PMIs were utilized for testing. We used the 80/20 training-test sets rule according to [68].

3.4. Training the system

We implemented a sequential model convolution neural network summarized in Fig. 6 using TensorFlow 2.1 [69]. The model consists of three convolutional layers with 32, 64, and 128 filter sizes and a kernel size of 3 accompanied by the hyperbolic tangent activation function. After each layer, batch normalization and average pooling layers are applied. The feature map obtained is flattened into 2048 one-dimension arrays as an imaging outcome which is connected to 1843 neurons using a dense layer accompanied by the sigmoid activation function. Then, 25% of the connected neurons are removed by a drop-out layer. Finally, the last dense layer provides 1024 probability distributions ranging from 0 to 1 applying the softmax activation function which is used to label the character codes. The model uses the root-mean-square error, the cross-entropy loss, and the accuracy as the optimizer, loss function, and performance metrics respectively. The CNN was trained on an i7-1165G7 @ 2.8 GHz laptop computer with 16 GB RAM and an NVIDIA GeForce MX450 GPU. Training time: 4' 18", after 30 epochs (case A) and 6' 23" after 40 epochs (case B). The obtained accuracy and loss values are shown in Table 1.

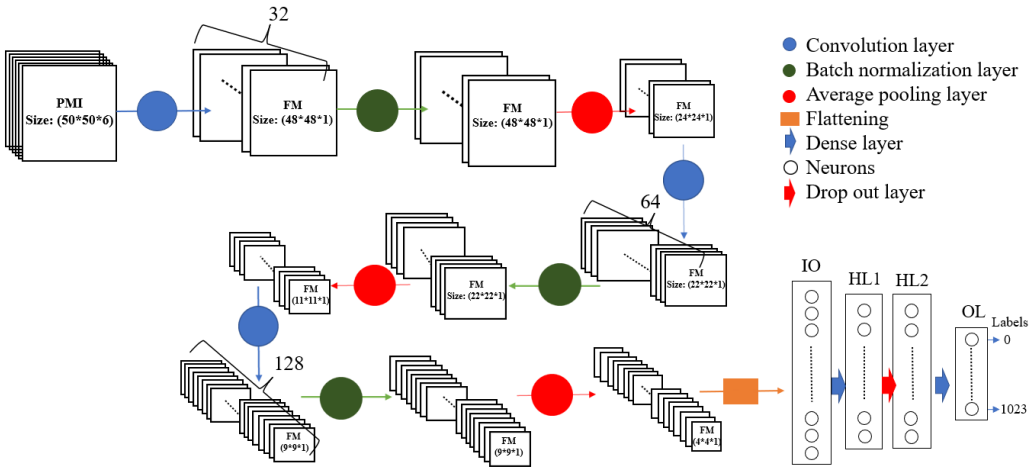


Figure 6: Neural network model: PMI, FM, IO, HL, and OL stand for polarization mapping image, feature-map, image-outcome, hidden layer, and output layer, respectively

		Accuracy	Loss
Case A, $\omega = \pi/8$	Training set	0.997	0.011
	Test set	0.967	
	Experimental	0.901	
Case B, $\omega = \pi/2$	Training set	0.992	0.028
	Test set	0.925	
	Experimental	0.921	

Table 1: Network accuracy and loss

4. Results and discussion

We optically tested the recognition capability of our approach using 210 randomly selected pairs of characters. One of the characters of the pair is optically processed with a polarization state equal to $\omega = \pi/8$ (case A) and subsequently detected by interrogating the CNN. The other one is processed the same way, but using polarization state equal to $\omega = \pi/2$ (case B). Then, the two detected characters are XOR-recombined to produce the visually-encrypted message. We found that the accuracy for polarization cases A and B is 0.901 and 0.921 respectively (see Table 1).

To sum up, we designed a successful optical setup and a coding procedure able to implement visual encryption. Some design variables can be modified to deploy alternative systems:

1. The characters are encoded assuming the longitudinal component E_z is described by the Fourier transform of the function $C(\varphi)$. Other implementations of $\mathbf{E_S}$ can be considered, provided the network is trained accordingly.
2. The system has been demonstrated using high NA microscope objectives and spiral polarization. However, low NA lenses or other polarizations could be used as well.
3. The character set used is limited to 1024 codes, but the method can be easily scaled to be used with binary codes of arbitrary length. In particular, the system can be able to be used with the complete Unicode set.
4. Radius R_0 and R_1 can be considered design variables. Any change in these values will produce a complete different training set. In section 3.1, we explained how R_1 and R_0 were selected. If the codes to be

optically analyzed use other radii values, it is very likely that recognition will not be possible. Figure 7 displays synthetically produced PMIs for code ň (U+0148) using different values for R_1 and R_0. In this example, we use spiral polarization (case A). The code and the corresponding PMI depicted on row (a) uses the same radii utilized for training the system. Rows (b), (c) and (d) shows the PMIs for different combinations of R_1 and R_0, as indicated in the caption of Fig. 7. As expected, these intensity patterns are slightly different and when these PMIs are used to interrogate the CNN, the network wrongly predicts codes (b), (c) and (d) as characters (U+01A5), (U+01A4) and (U+03D4), respectively.

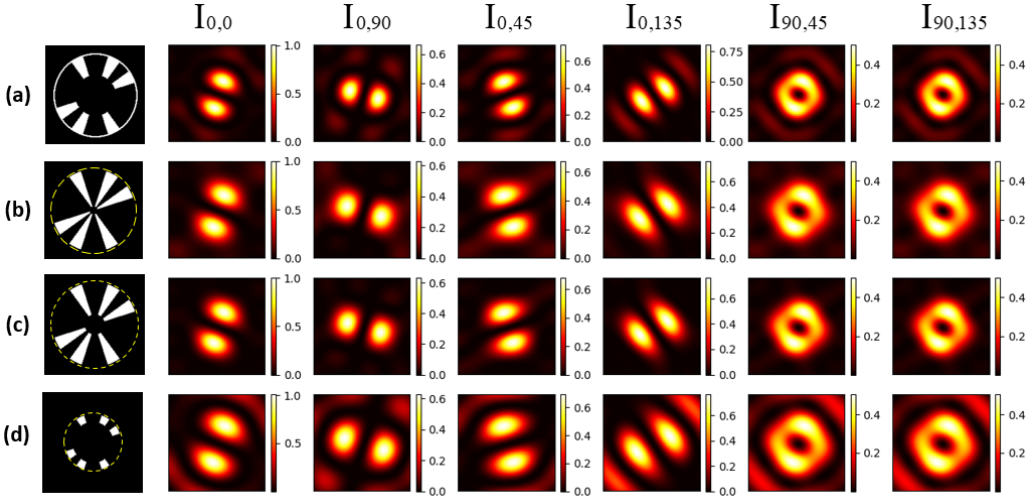


Figure 7: PMIs for code ň (U+0148) generated with different radii and using system A (spiral polarization): (a) R_1=3.75 mm and R_0=1.8 mm. (b) R_1=3.75 mm and R_0=0.36 mm (c) R_1=3.75 mm and R_0=0.9 mm (d) R_1=2.5 mm and R_0.

5. It is worth considering that the neural network will provide a correct answer only if the six polarimetric channels of the PMI are available. In general, if an attacker is not able to access the complete group of polarimetric images, they will not be able to recover the expected character. This means that the number of recipients involved might be increased up to twelve.
   In order to justify this statement, we show the accuracy results when one of the channels of the PMI contains only random values (see table

2): Accuracy values are almost zero when one of the channels ($I_{0,0}$, $I_{0,45}$, $I_{0,90}$, or $I_{0,135}$) do not provide information.
Since the system is illuminated with non-uniform linear polarized light (radial or spiral), the contribution of channels $I_{90,45}$ and $I_{90,135}$ is less critical for the recognition process. Interestingly, if we simultaneously remove the information of the $I_{90,45}$ and $I_{90,135}$ channels, the accuracy value depends on the polarization of the illuminating beam. When radial polarization is used, it is enough to utilize the channel set ($I_{0,0}, I_{0,45}, I_{0,90}, I_{0,135}$) to get a high accuracy value. However, this is no longer true for spiral polarization. In general, to avoid false recognition, it is required not to ignore any channel.

Channel missing	Case A (spiral)	Case B (radial)
$I_{0,0}$	0.012	0.014
$I_{0,90}$	0.012	0.014
$I_{0,45}$	0.026	0.038
$I_{0,135}$	0.008	0.056
$I_{90,45}$ and $I_{90,135}$	0.436	0.960

Table 2: Test accuracy for channels containing random information. Test data-set: 500 codes.

6. We have also considered the effect of using the channels of the interrogating PMI in the wrong order. PMIs of the training set were built considering the following order: $I_{0,0}, I_{0,90}, I_{0,45}, I_{0,135}, I_{90,45}, I_{90,135}$. Table 3 displays some accuracy results when the channels of the PMIs of the test set are not provided in the appropriate order. Results clearly demonstrate that the system becomes unreliable if testing PMIs are not arranged according to the design.

	Case A (spiral)	Case B (radial)
$I_{0,90}, I_{0,0}, I_{0,45}, I_{0,135}, I_{90,45}, I_{90,135}$	0.004	0.006
$I_{0,0}, I_{0,90}, I_{0,135}, I_{0,45}, I_{90,45}, I_{90,135}$	0.010	0.020
$I_{0,45}, I_{0,90}, I_{0,0}, I_{0,135}, I_{90,45}, I_{90,135}$	0.304	0.120
$I_{0,135}, I_{0,45}, I_{0,90}, I_{0,0}, I_{90,45}, I_{90,135}$	0.010	0.006

Table 3: Test accuracy for PMI channels provided in the wrong order.

7. Occlusion attack is a common test in optical encryption. To produce a suitable visual encryption system, we designed our CNN to be efficient for pattern recognition and classification purposes. When the present CNN is tested against PMIs with blocked information, accuracy results worsen fast. To test the behavior of the network, we produced three 500-character PMI test-sets. Every set contains no information in continuous areas equivalent to 6% (set O1), 10% (set O2) and 16% (set O3) of the total pixels. The corresponding accuracy results are shown in Table 4: when the area occluded is below 10%, the CNN performs well, but above this point, accuracy decreases fast. For illustrative purposes, examples of partially occluded $I_{0,0}$ elements that belong to set O3 are shown in Fig. 8.
   To successfully circumvent this attack, our network could be trained using a large set of occluded PMIs. This methodology is equivalent to the proposed design of PMIs to avoid noise.

Test set	Case A (spiral)	Case B (radial)
Set O1: Area occluded: 6%	0.974	0.976
Set O2: Area occluded: 10%	0.980	0.974
Set O3: Area occluded: 16%	0.820	0.810

Table 4: Test accuracy for PMIs containing occluded information. Test data-set: 500 codes.

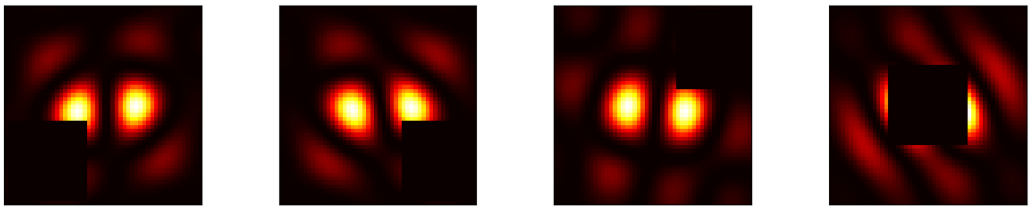


Figure 8: Partially occluded (16%) channel $I_{0,0}$ for codes d (U+0064), È (U+00C8), Ĭ (U+012C) and U+0190, generated using radial polarization

5. Concluding remarks

We have introduced an optical approach for implementing visual encryption for a set of optical codes. The system is based on a holographic optical

setup able to record polarimetric images of the irradiance at the focal plane of an objective lens. The character to be analyzed is encoded and optically processed, producing the aforementioned polarimetric images. These distributions are used to interrogate a CNN that is able to determine the corresponding code. Interestingly, the network will only provide correct results if it has been trained with the proper polarization state and the precise knowledge of radius R_1 and R_2 for designing the CE.

We found that visual encryption of 10 bit Unicode characters was possible with a very high success rate. Despite the group of characters used is small, our technique can be easily scaled to consider, for instance, the full 16-bit Unicode set. Also, we demonstrated the use of visual encryption using two shares. Note that the six polarimetric images should be provided to the recipients. Since the CNN requires the complete group to provide accurate results, the number of recipients involved might be increased up to twelve. Despite the network was not designed to be used with occluded information, accuracy performance is good enough when the percentage of blocked pixels is not higher than 10%.

Credit author statement

Kavan Ahmadi: Conceptualization, Methodology, Data curation, Formal analysis, Software, Investigation, Writing-Original draft. **Artur Carnicer:** Conceptualization, Writing-Reviewing and Editing, Supervision.

Acknowledgments

The authors are indebted to Prof. David Maluenda for enlightening discussions.

Funding

This work was supported by Ministerio de Ciencia e Innovation, project PID2019-104268GB-C22 / AEI / 10.13039/501100011033. KA acknowledges financial support provided by the PREDOCS-UB program.

Declaration of competing interest

The authors declare no competing interests.

References

[1] B. Javidi, J. L. Horner, Optical pattern recognition for validation and security verification, Opt. Eng. 33 (6) (1994) 1752–1756.

[2] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (7) (1995) 767–769.

[3] O. Matoba, B. Javidi, Encrypted optical memory system using three-dimensional keys in the Fresnel domain, Opt. Lett. 24 (11) (1999) 762–764.

[4] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett. 29 (14) (2004) 1584–1586.

[5] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (12) (2000) 887–889.

[6] B. Hennelly, J. T. Sheridan, Optical image encryption by random shifting in fractional Fourier domains, Opt. Lett. 28 (4) (2003) 269–271.

[7] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image. Vis. Comput. 24 (9) (2006) 926–934.

[8] W. Qin, X. Peng, Asymmetric cryptosystem based on phase-truncated Fourier transforms, Opt. Lett. 35 (2) (2010) 118–120.

[9] B. Javidi, T. Nomura, Securing information by use of digital holography, Opt. Lett. 25 (1) (2000) 28–30.

[10] E. Tajahuerce, B. Javidi, Encrypting three-dimensional information with digital holography, Appl. Opt. 39 (35) (2000) 6595–6601.

[11] Y. Zhang, B. Wang, Optical image encryption based on interference, Opt. Lett. 33 (21) (2008) 2443–2445.

[12] X. Meng, L. Cai, X. Xu, X. Yang, X. Shen, G. Dong, Y. Wang, Two-step phase-shifting interferometry and its application in image encryption, Opt. Lett. 31 (10) (2006) 1414–1416.

[13] G. Situ, J. Zhang, Multiple-image encryption by wavelength multiplexing, Opt. Lett. 30 (11) (2005) 1306–1308.

[14] P. Clemente, V. Durán, E. Tajahuerce, J. Lancis, et al., Optical encryption based on computational ghost imaging, Opt. Lett. 35 (14) (2010) 2391–2393.

[15] W. Chen, X. Chen, C. J. Sheppard, Optical image encryption based on diffractive imaging, Opt. Lett. 35 (22) (2010) 3817–3819.

[16] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, S. Liu, Double image encryption by using iterative random binary encoding in gyrator domains, Opt. Express 18 (11) (2010) 12033–12043.

[17] B. Javidi, T. Nomura, Polarization encoding for optical security systems, Opt. Eng. 39 (9) (2000) 2439–2443.

[18] A. Alfalou, C. Brosseau, Dual encryption scheme of images using polarized light, Opt. Lett. 35 (13) (2010) 2185–2187.

[19] E. Pérez-Cabré, M. Cho, B. Javidi, Information authentication using photon-counting double-random-phase encrypted images, Opt. Lett. 36 (1) (2011) 22–24.

[20] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys, Opt. Lett. 30 (13) (2005) 1644–1646.

[21] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (8) (2006) 1044–1046.

[22] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express 15 (16) (2007) 10253–10265.

[23] J. Chen, X.-W. Li, Q.-H. Wang, Deep learning for improving the robustness of image encryption, IEEE Access 7 (2019) 181083–181091.

[24] L. Zhou, Y. Xiao, W. Chen, Machine-learning attacks on interference-based optical encryption: experimental demonstration, Opt. Express 27 (18) (2019) 26143–26154.

[25] L. Chen, B. Peng, W. Gan, Y. Liu, Plaintext attack on joint transform correlation encryption system by convolutional neural network, Opt. Express 28 (19) (2020) 28154–28163.

[26] L. Zhou, Y. Xiao, W. Chen, Vulnerability to machine learning attacks of optical encryption based on diffractive imaging, Opt. Laser Eng. 125 (2020) 105858.

[27] L. Zhou, Y. Xiao, W. Chen, Learning complex scattering media for optical encryption, Opt. Letters 45 (18) (2020) 5279–5282.

[28] H. Wu, X. Meng, X. Yang, X. Li, P. Wang, W. He, H. Chen, Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination based deep-learning correlography, Opt. Laser Eng. 138 (2021) 106454.

[29] X. Wang, H. Wei, Cryptanalysis of compressive interference-based optical encryption using a U-Net deep learning network, Opt. Commun. 507 (2022) 127641.

[30] F. Wang, R. Ni, J. Wang, Z. Zhu, Y. Hu, Invertible encryption network for optical image cryptosystem, Opt. Laser Eng. 149 (2022) 106784.

[31] A. Alfalou, C. Brosseau, Optical image compression and encryption methods, Adv. Opt. Photonics 1 (3) (2009) 589–636.

[32] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, B. Javidi, Optical techniques for information security, Proc. IEEE 97 (6) (2009) 1128–1148.

[33] W. Chen, B. Javidi, X. Chen, Advances in optical security systems, Adv. Opt. Photonics 6 (2) (2014) 120–155.

[34] S. Liu, C. Guo, J. T. Sheridan, A review of optical image encryption techniques, Opt. Laser Technol. 57 (2014) 327–342.

[35] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, et al., Roadmap on optical security, J. Opt. 18 (8) (2016) 083001.

[36] N. K. Nishchal, Optical cryptosystems, IOP Publishing, 2019.

[37] Q. Zhan, Cylindrical vector beams: from mathematical concepts to applications, Adv. Opt. Photonics 1 (1) (2009) 1–57.

[38] A. Carnicer, B. Javidi, Optical security and authentication using nanoscale and thin-film structures, Adv. Opt. Photonics 9 (2) (2017) 218–256.

[39] K. Ahmadi, P. Latorre-Carmona, B. Javidi, A. Carnicer, Polarimetric identification of 3D-printed nano particle encoded optical codes, IEEE Photon. J. 12 (3) (2020) 1–10.

[40] A. Fatima, N. K. Nishchal, Image authentication using a vector beam with sparse phase information, J. Opt. Soc A. A 35 (6) (2018) 1053–1062.

[41] A. Fatima, N. K. Nishchal, Optical image security using stokes polarimetry of spatially variant polarized beam, Opt. Commun. 417 (2018) 30–36.

[42] Q. Wang, D. Xiong, A. Alfalou, C. Brosseau, Optical image authentication using spatially variant polarized beam and sparse phase sampling method, Opt. Lasers Eng. 124 (2020) 105828.

[43] P. Kumar, A. Fatima, N. K. Nishchal, Arbitrary vector beam encoding using single modulation for information security applications, IEEE Photon. Technol. Lett. 33 (5) (2021) 243–246.

[44] M. Tzoufras, F. Tsung, W. Mori, A. Sahai, Improving the self-guiding of an ultraintense laser by tailoring its longitudinal profile, Phys. Rev. Lett. 113 (24) (2014) 245001.

[45] L. Kallioniemi, L. Turquet, H. Lipsanen, M. Kauranen, G. Bautista, Tailoring the longitudinal electric fields of high-order laser beams and their direct verification in three dimensions, Opt. Commun. 459 (2020) 124894.

[46] A. Carnicer, I. Juvells, B. Javidi, R. Martínez-Herrero, Optical encryption in the longitudinal domain of focused fields, Opt. Express 24 (7) (2016) 6793–6801.

[47] A. Carnicer, I. Juvells, B. Javidi, R. Martínez-Herrero, Optical encryption in the axial domain using beams with arbitrary polarization, Opt. Lasers Eng. 89 (2017) 145–149.

[48] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[49] M. Naor, A. Shamir, Visual cryptography, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 1–12.

[50] J. Han, C.-S. Park, D.-H. Ryu, E.-S. Kim, Optical image encryption based on XOR operations, Opt. Eng. 38 (1) (1999) 47–54.

[51] Y. Qin, Y. Zhang, Information encryption in ghost imaging with customized data container and XOR operation, IEEE Photon. J. 9 (2) (2017) 1–8.

[52] P. Kumar, A. Fatima, N. K. Nishchal, Image encryption using phase-encoded exclusive-or operations with incoherent illumination, J. Opt. 21 (6) (2019) 065701.

[53] P. Kumar, N. K. Nishchal, Enhanced exclusive-or and quick response code-based image encryption through incoherent illumination, Appl. Opt. 58 (6) (2019) 1408–1412.

[54] T. Zhao, Y. Chi, A novel secret sharing with two users based on joint transform correlator and compressive sensing, J. Mod. Opt. 65 (9) (2018) 1072–1080.

[55] T. Zhao, Y. Chi, Secret image sharing based on multiphase retrieval algorithm, J. Mod. Opt. 67 (15) (2020) 1296–1303.

[56] D. Lu, M. Liao, W. He, Q. Xing, G. Verma, X. Peng, Experimental optical secret sharing via an iterative phase retrieval algorithm, Opt. Lasers Eng. 126 (2020) 105904.

[57] X. Liu, X. Meng, Y. Wang, H. Wu, X. Yang, W. He, H. Chen, Optical multilevel authentication based on singular value decomposition ghost imaging and secret sharing cryptography, Opt. Lasers Eng. 137 (2021) 106370.

[58] Y. LeCun, L. Bottou, Y. Bengio, P. Haffner, Gradient-based learning applied to document recognition, Proc. IEEE 86 (11) (1998) 2278–2324.

[59] B. Richards, E. Wolf, Electromagnetic diffraction in optical systems, II. structure of the image field in an aplanatic system, Proc. R. Soc. Lond. A Math. Phys. Sci. 253 (1274) (1959) 358–379.

[60] L. Novotny, B. Hecht, Principles of nano-optics, Cambridge University, 2012.

[61] V. Arrizón, Complex modulation with a twisted-nematic liquid-crystal spatial light modulator: double-pixel approach, Opt. Lett. 28 (15) (2003) 1359–1361.

[62] K. Ahmadi, D. Maluenda, A. Carnicer, Fast mapping of double-pixel holograms using k-nearest neighbors, in: Digital Holography and Three-Dimensional Imaging, Optical Society of America, 2021, pp. DW5E–7.

[63] E. Perez-Cabre, B. Javidi, Scale and rotation invariant optical id tags for automatic vehicle identification and authentication, IEEE Trans. Veh. Technol. 54 (4) (2005) 1295–1303.

[64] CNN, The inspiring hidden message in the mars perseverance rover's parachute, `https://edition.cnn.com/2021/02/22/world/mars-rover-new-video-images-scn-trnd/index.html` (2021).

[65] D. Maluenda, R. Martínez-Herrero, I. Juvells, A. Carnicer, Synthesis of highly focused fields with circular polarization at any transverse plane, Opt. Express 22 (6) (2014) 6859–6867.

[66] D. Maluenda, M. Aviñoá, K. Ahmadi, R. Martínez-Herrero, A. Carnicer, Experimental estimation of the longitudinal component of a highly focused electromagnetic field, Sci. Rep. 11 (1) (2021) 1–10.

[67] K. Ahmadi, Beam implementation with a translucent twisted-nematic liquid crystal display, in: P. J. Rosen (Ed.), Holography - Recent Advances and Applications, IntechOpen, Rijeka, 2022, Ch. 25. `doi:10.5772/intechopen.105671`.
URL `https://doi.org/10.5772/intechopen.105671`

[68] A. Gholamy, V. Kreinovich, O. Kosheleva, Why 70/30 or 80/20 relation between training and testing sets: A pedagogical explanation, Departmental Technical Reports (CS). The University of Texas at El Paso (2018).

[69] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard, Y. Jia, R. Jozefowicz, L. Kaiser, M. Kudlur, J. Levenberg, D. Mané, R. Monga, S. Moore, D. Murray, C. Olah, M. Schuster, J. Shlens, B. Steiner, I. Sutskever, K. Talwar, P. Tucker, V. Vanhoucke, V. Vasudevan, F. Viégas, O. Vinyals, P. Warden, M. Wattenberg, M. Wicke, Y. Yu, X. Zheng, TensorFlow: Large-scale machine learning on heterogeneous systems, software available from tensorflow.org (2015).
URL `https://www.tensorflow.org/`