Hybrid optical-digital encryption system based on wavefront coding paradigm

Mikhail V. Konnik
School of Electrical Engineering and Computer Science,
The University of Newcastle, Callaghan 2308 Australia

ABSTRACT
The wavefront coding is widely used in the optical systems to compensate aberrations and increase the depth of field. This paper presents experimental results on application of the wavefront coding paradigm for data encryption. We use a synthesised diffractive optical element (DOE) to deliberately introduce a phase distortion during the images registration process to encode the acquired image. In this case, an optical convolution of the input image with the point spread function (PSF) of the DOE is registered. The encryption is performed optically, and is therefore fast and secure. Since the introduced distortion is the same across the image, the decryption is performed digitally using deconvolution methods. However, due to noise and finite accuracy of a photosensor, the reconstructed image is degraded but still readable.

The experimental results, which are presented in this paper, indicate that the proposed hybrid optical-digital system can be implemented as a portable device using inexpensive off-the-shelf components. We present the results of optical encryption and digital restoration with quantitative estimations of the images quality. Details of hardware optical implementation of the hybrid optical-digital encryption system are discussed.

Keywords: wavefront coding, optical encryption system, digital decryption, hybrid systems

1. INTRODUCTION
The encryption systems operating in the optical domain are attractive due to inherent parallelism and speed of optical systems. The advantages of optical encryption systems, such as a high speed, high level of security, and the difficulty of accessing or falsification are widely recognised.

The optical encryption systems can be divided on three broad categories: mostly optical, mostly digital, and hybrid optical-digital systems. Digital encryption systems perform all operations numerically as a computer program\(^1\) so there is no need of optical systems to be created. Examples of such mostly digital systems are Virtual Optics system,\(^2\) virtual-optical-holography (VOH),\(^3\) and encryption systems based on fractional wavelet\(^4\) or fractional Fourier transform.\(^5\) The digital encryption systems are characterised by high cryptography resistance, low cost, and flexibility. The drawbacks include a significant amount of data and considerable computation power. On the other hand, mostly optical encryption techniques use a high speed and parallelism of optical images processing. The most widespread approach in optical encryption systems is double random phase mask.\(^6–9\) Such systems allow obtaining encrypted images that are characterised by high cryptography resistance. Images are being encrypted in a very short time because of parallel optical processing. Complexity of optical scheme and expensiveness are drawbacks of such systems. Moreover, several vulnerabilities of double random phase mask were reported recently.\(^10–12\)

In this paper we present an alternative encryption approach, where the encryption is performed optically using “wavefront coding”\(^13\) or “pupil engineering”\(^14\) paradigm, and the decryption is performed digitally using deconvolution algorithms. Such a hybrid optical-digital systems allow combining advantages of optical processing (high speed and parallelism) and digital processing (flexibility of digital image processing methods). The known distortions are deliberately introduced in the registered image and used for enhancing depth of field in

Further author information: Mikhail V. Konnik, mail@mvkonnik.info
microscopic imaging,\textsuperscript{15} aberrations compensation,\textsuperscript{16} depth-of-field improvement in MEMS-systems,\textsuperscript{17} and enhancing of tomography images.\textsuperscript{18} Digital images deconvolution is performed in order to reconstruct the image and compensate the introduced distortions.

Hybrid optical-digital systems based on “wavefront coding” and “pupil engineering” paradigms can be used not only for images enhancing, but for optical encryption, too. We use synthesised diffractive optical elements (DOE) to deliberately introduce a phase distortion in the registered images to encrypt them. Since the introduced distortion is the same across the image, the reconstruction is performed digitally using deconvolution algorithms. The experimental results show that the proposed hybrid optical-digital system can be implemented as a portable device using inexpensive off-the-shelf components. The decoded images are of lower quality than the original due to photosensor noise and imperfections of the DOE. Nonetheless, such a hybrid optical-digital system can be regarded as a reliable and portable solution for information security.

2. OPTICAL ENCRYPTION BASED ON THE WAVEFRONT CODING

The method of diffractive optical coding is based on the assumption of linearity of the system and the concept of a convolution. The coding scheme is shown in Fig. 1. The object is illuminated by a spatially incoherent monochromatic light with a wavelength $\lambda$. When the light passes through a diffractive optical element (DOE), the convolution of the object’s image with the point spread function (PSF) of the DOE is performed. The resulting convolution is recorded by a photosensor in the registration plane $(x_i, y_i)$ and represents an encoded (encrypted) image.

2.1 Mathematical formulation of the encoding process

A mathematical model of optical coding is based on the concept of a convolution. Assume that the encoded image is at a distance of $d_0$ in front of a camera (see Fig. 1) and is illuminated by spatially incoherent laser light. Denote $d_i$ the distance from the camera lens to a sharp image in the recording plane, where the photosensor is located. Denote $I_0(x_0, y_0)$ the intensity distribution in the plane of the input scene.

In case when the DOE is not used in image formation process, the intensity distribution in the input plane for registration is $f(x, y) = \frac{1}{M^2} I_0(\frac{x}{M}, \frac{y}{M})$. In this case, we can denote $M = d_i/d_0$ the magnification of the optical system.

![Figure 1. Scheme of optical encryption based on the wavefront coding.](image_url)
$f(x, y)$ with the PSF of the DOE $h(x, y)$ is registered in the registration plane $(x_i, y_i)$:

$$g(x, y) = f(x, y) \otimes h(x, y),$$

where PSF of the DOE can be represented as:

$$h(x, y) = \frac{1}{\lambda d_D} \int \int dx_D dy_D t(x_D, y_D) e^{i 2 \pi \left( \frac{x x_D}{\lambda d_D} + \frac{y y_D}{\lambda d_D} \right)} \right)^2,$$

where $t(x_D, y_D)$ is amplitude-phase transmission function of the DOE at the wavelength $\lambda$, $x_D$ and $y_D$ are the coordinates in the plane of the DOE.

Denote $r(x_D, y_D) = h(x, y)$ a PSF of the DOE, which is convoluted with the input scene image $I_0(x_0, y_0)$. The convolution $g(x, y)$ of the input scene image $f(x, y)$ and the PSF of the DOE $r(x_D, y_D)$ can be therefore represented as:

$$g(x, y) = \frac{1}{M^2} I_0 \left( \frac{x}{M} \right) \otimes r \left( \frac{x}{\lambda d_D}, \frac{y}{\lambda d_D} \right).$$

The dependence of the DOE’s PSF $r(x_D, y_D)$ on $\lambda$ means that the image of the PSF will scale with different wavelength of a light. Thus the output of such an optical system (a convolution), which is registered by a solid photosensor, is the intensity distribution of the convolution of the input scene image with the PSF DOE.

### 2.2 Formulation of decoding by digital deconvolution

The optical encoding (based on the optical convolution) is described as:

$$g(x, y) = f(x, y) \otimes h(x, y) + n(x, y),$$

where $g(x, y)$ is the encrypted image, $f(x, y)$ is the original image, $h(x, y)$ is the point spread function (PSF) of the DOE, and $n(x, y)$ is the additive noise. In the Fourier domain the Eq.4 can be rewritten as:

$$G(u, v) = F(u, v) \cdot H(u, v) + N(u, v).$$

In the absence of noise, the decoded image (deconvolution) will be found as:

$$\hat{F}(u, v) \approx \frac{G(u,v)}{H(u,v)} = G(u,v) \cdot Y(u,v),$$

where $Y(u, v)$ is the decryption key (restoration function). However, a pure deconvolution with $Y(u, v) = \frac{1}{H(u,v)}$ is not appropriate in the presence of noise, which is inevitably added in the registration process.

A better solution to the deconvolution problem is to use of regularisation methods. In this type of hybrid optical-digital systems, both one-step and iterative deconvolution algorithms can be used. In our previous report\textsuperscript{19} we have shown that the *evolutionary*\textsuperscript{*} deconvolution algorithm provides slightly better restoration. The mathematical formulation of the evolutionary deconvolution algorithm is as follows:

$$Y(u,v,\sigma,\mu,\theta) = \left( \frac{H(u,v)}{|H(u,v)|^2} \right)^\sigma \cdot \left( \frac{|H(u,v)|^2}{|H(u,v)|^2 + \theta \cdot Q(u,v)} \right)^\mu,$$

where $\theta$ is the regularisation parameter, $\sigma$ and $\mu$ are the inversion and smoothing parameters, respectively. Further comparison of one-step methods can be found in.\textsuperscript{19}

\textsuperscript{*}The name *evolutionary* for such a deconvolution algorithm refers to the following. With different values of parameters $\sigma$ and $\mu$, the algorithm can vary, or evolve, from the inverse $[\sigma = 1$ and $\mu = 0]$ to Wiener-like $[\sigma = 1$, $\mu = 1$, and $\theta = 10^{-1} \ldots 10^{-10}]$ deconvolution.
3. EXPERIMENTAL SETUP OF THE OPTICAL ENCRYPTION SYSTEM BASED ON THE WAVEFRONT CODING

The encryption is performed optically; hence we have to use diffractive optical elements (DOE) that contain an encryption key. The usual choice for the DOE is Fourier holograms. However, Fourier holograms have several diffraction orders, which makes it difficult to use the Fourier holograms in optical-digital systems. An alternative solution is to use synthesised holograms, particularly the diffractive phase elements as a kinoform. The kinoform performs only the phase modulation of the light and its impulse response contains the only one diffraction order. Another advantage of kinoforms is their high diffraction efficiency that is close to 100%. Kinoforms can be synthesised as a phase grating using Gerchberg-Saxton or Fienup methods.

The experimental setup for optical encoding is shown in Fig. 2. The light from the YAG:Nd laser is attenuated by a polariser and is focused by a micro lens. The light is passed through the spatial frequency filter to make the illumination more uniform. The spatial coherence of laser light is destroyed by a rotating ground glass to reduce the influence of speckle noise. Light reflected from the input scene is recorded by a digital camera. The kinoform is placed inside the camera space between the lens and the photosensor. Computer controls the process of image acquisition and can perform the digital decryption of images.

![Figure 2. Experimental setup of optical encryption: 1 - laser YAG:Nd crystal with KDP, 2 - attenuation filter, 3 - micro lens, 4 - spatial frequency filter, 5 - a rotating ground glass for the destruction of spatial coherence of laser light, 6 - the input scene being encrypted, 7 - digital camera, 8 - DOE (kinoform), 9 - computer.](image)

The scale of the PSF of a DOE depends on the wavelength $\lambda$ of the light (see Eq.3) is used for the encryption process. The correct scale of the PSF can be calculated or (which is better) registered optically. The optical scheme of the experimental setup must be modified for the registration of the PSF, as shown in Fig. 3. Since the encryption system is based on the convolution, the PSF can be registered by convolution of the DOE’s PSF with the Dirac’s Delta function (a bright point light source).

![Figure 3. The experimental setup for the registration of the kinoform’s PSF: 1 - light source, 2 - opaque light screen, 3 - fibre, 4 - DOE (kinoform), 5 - digital camera, 6 - PC.](image)

A typical scheme for the PSF registration is presented in Fig. 3. The light from the YAG:Nd laser passes through the light attenuator and enters the waveguide (fibre). The convolution of the PSF of the DOE with a point source of light is registered by the digital camera. The image of the PSF is transferred to computer.
3.1 The parameters of the optical setup

We use the DOE (kinoform) that is synthesised by Gerchberg-Saxton algorithm and manufactured as a phase mask etched on the plastic disk. The typical size of a DOE used in this work is ø5 mm. The PSF image of the DOE was of size 320 × 270 pixels after the registration by the digital camera. The PSF was registered using a point light source formed by a solid-state YAG:Nd laser $\lambda = 0.53 \mu m$.

Digital camera used for the registration of encrypted images is Canon EOS 400D with a Bayer colour filter array and CMOS photosensor with 3888 × 2592 pixels. The ADC of the camera is 12-bit and the physical size of photosensor pixels $5.7 \times 5.7 \mu m^2$. The light source was a YAG:Nd laser with a wavelength $\lambda = 0.53 \mu m$ (with KDP doubling). Due to presence of Bayer filter on the photosensor, we use green pixels only. Therefore, the effective number of pixels was 1944 × 1296 with an effective pixel size of $11.4 \times 11.4 \mu m^2$.

3.2 The choice of a digital camera for registration of optically encrypted images

Because the image that is registered by the camera is a convolution rather than an original image, the correct registration of half-tones is crucial. The usual choice for the images acquisition is industrial-grade or scientific grade cameras. However, modern consumer-grade SLR cameras have achieved a remarkable level of images quality and therefore can be used as components of optical systems. Using special software converters, one can obtain linear, raw, and undistorted images from those consumer-grade cameras just like from scientific- or industrial-grade cameras. It was shown that the signal-to-noise ratio of modern consumer-grade cameras can exceed the industrial-grade cameras. Furthermore, the portability and power efficiency of consumer-grade cameras make them ideal for the portable optical encryption systems. All the results reported in this paper were obtained on the consumer-grade camera Canon EOS 400D; however, most modern SLR cameras as well as industrial or scientific-grade cameras can be used as well.

4. EXPERIMENTAL RESULTS ON OPTICAL ENCRYPTION

In order to simplify the analysis of the decrypted images quality, the test scenes for the encryption contained a text printed on a paper. The text was typesetted in Courier New Cyr Bold font of size 16, 14, 12 and 10 pt. When the text is printed and registered by a camera (without encryption), the text element corresponds to 30 × 30, 25 × 25, 20 × 20, and 18 × 18 pixels. Minimal text element in this case was chosen as a letter “e”.

The images acquired by digital camera were of size 3888 × 2592 pixels, and only the green pixels were used. Registered images of test samples (encryption DOE is removed) are shown in Fig. 4.

Figure 4. The original images (text samples attached to the input scene) with the minimal text element: a) 30 × 30 pixels correspond to 16 pt text, b) 25 × 25 pixels correspond to 14 pt text, c) 20 × 20 pixels correspond to 12 pt text, d) 18 × 18 pixels correspond to 10 pt text.

The registration of the DOE’s PSF has to be performed in order to decrypt the optically encoded images. The images of the PSF were registered using the experimental setup shown in Fig. 3. Since the consumer-grade camera was used as a acquisition device, the images were processed (“linearised”) using software converter dcraw as described in. The PSF image that registered in conventional camera mode (as a photo) is of poor contrast and non-linear (see Fig. 4a). On the other hand, the image of the PSF, which has been processed by the software converter dcraw, is linear and therefore with correct half-tones (see Fig. 4b).
The original test images (see Fig. 4) were optically encrypted using the encryption key (the PSF of the DOE) presented in Fig. a. The encrypted images are shown in Fig. 6.

The results of digital decryption of the optically encrypted images are presented in the further section.

5. EXPERIMENTAL RESULTS ON DIGITAL DECRYPTION OF THE OPTICALLY CODED IMAGES

The test samples, which were printed on a paper and attached to the input scene, were optically encrypted (see Fig. 6) and registered by the digital camera. Using digital deconvolution algorithms (previously reported in\textsuperscript{19}) and the image of the DOE’s PSF (see Fig. 4), which was used as an encryption key, one can decode the encrypted message by the deconvolution. Since the optical convolution (an encrypted image) was registered by a camera, the noise was inevitably added to the resulting convolution. Therefore, the decrypted image will be noised and some letters distorted.

The results of the decryption are presented below. Both qualitative (visually best image in the group) and quantitative (normalised root mean squared error, NRMSE) measures of the images quality were used.

5.1 Test sample with text elements of 25 × 25 pixels

The test sample with the letters of 14 pt size (text element on the image occupies 25 × 25 = 625 pixels). The optically coded images were decrypted with the “evolution” digital deconvolution algorithm with different regularisation parameters values $\theta$. The decrypted images are presented in Fig. 7.

One can see from Fig. 7a that the excessive values of regularisation parameter $\theta$ lead to blurred decoded images that are hard to read. The visually best image in the group (see Fig. 7b) is readily identifiable despite some distortions on the bottom of the images. The decoded image appears noised and unreadable when the regularisation in insufficient, as shown in Fig. 7c.
5.2 Test sample with text elements of 20 × 20 pixels

Next, the test samples with the letters of 12 pt size (text element on the registered image occupies 20 × 20 pixels). The optically coded images were decrypted with the same digital deconvolution algorithm and different values of the regularisation parameter \( \theta \) (see Fig. 9). As before, three images are provided for the comparison: with excessive regularisation parameter \( \theta \) (see Fig. 9a), the visually best image in the group (see Fig. 9b), and the image decrypted with insufficient regularisation parameter \( \theta \) (see Fig. 9c). According to the NRMS error metric, the image with the minimal error from the original of 0.27 (the best in the NRMSE sense) was decrypted with the regularisation parameter \( \theta = 10^{-5} \), as shown in Fig. 10a. It should be noted that with decreasing size of the text elements of the encrypted images, the impact of the lack of regularisation will be more prominent.

The visual quality of the decrypted images from the optically encoded image in this case (the message of 12 pt text size with the 20 × 20 pixels letter size after registration) should be regarded as good: the text elements of the image are restored successfully despite the presence of image distortion at the bottom.

† The nature of those distortions of the decoded images can be attributed to lens imperfections, especially for uncompensated defocus and/or astigmatism. Such issues are the topic of current research.
5.3 Test sample with text elements of 18 × 18 pixels

At last, the test samples with the letters of 10 pt size were encrypted optically with the same PSF of the DOE (the letter of the text occupies 18 × 18 = 324 pixels on the registered image). The optically coded images were digitally decrypted with the same deconvolution algorithm. The decrypted images are presented below for the cases of the excessive regularisation parameter $\theta$ (see Fig. 11a), the visually best image in the group (see Fig. 11b), and the image decrypted with insufficient regularisation parameter $\theta$ (see Fig. 11c).

In this case (the size of the text is 10 pt) both visual quality and the NRMSE is worse than in the previous case (12 pt text size). The NRMSE of the visually best decrypted image in the group (see Fig. 11b) is 0.39 that can be considered tolerable.
The quantitative evaluation of the decoded images quality is shown in Fig. 12. The visually best image in the group (decrypted with the regularisation parameter $\theta = 10^{-5}$, NRMSE 0.39). However, the best decrypted image in the RMS sense was obtained with the regularisation parameter $\theta = 10^{-6}$ and NRMSE of 0.38.

Figure 12. Quantitative evaluation of the quality of the reconstructed images: a) the dependence of the RMS value versus the regularisation parameter $\theta$, lower is better; b) the decoded image with the minimum RMS error of 0.38 for the regularisation parameter $\theta = 10^{-6}$.

Overall, the quality of the decrypted images in this case can be considered as satisfactory because the noise and the distortions in the lower part of the decrypted image are stronger.

5.4 Results discussion

From the presented experimental data one can conclude that such type of optical encryption and digital decoding works like a lossy compression. The introduction of diffractive optical elements leads to a decrease in resolution of the decrypted images. Moreover, the photosensor inevitably adds the noise in the registered convolution of the input scene image and the PSF image of the DOE. As the number of pixels per one information element (a letter of a text in this case) decreases, the normalised root mean square error (NRMSE) increases. Therefore, the visual quality of decrypted image will deteriorate as the information element become smaller. The quantitative results on the images decryption are summarised in Table 1.

Table 1. The summary of the experimental results: digital decryption of optically encrypted images.

<table>
<thead>
<tr>
<th>The size of a text being optically encrypted, in pt</th>
<th>Pixels per information element Width X Height</th>
<th>NRMSE from the original image</th>
<th>The optimal value of the regularisation parameter $\theta$ for digital deconvolution by NRMSE</th>
<th>visually best</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>$30 \times 30$</td>
<td>0.24</td>
<td>$10^{-3}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>14</td>
<td>$25 \times 25$</td>
<td>0.25</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>12</td>
<td>$20 \times 20$</td>
<td>0.27</td>
<td>$10^{-5}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>10</td>
<td>$18 \times 18$</td>
<td>0.38</td>
<td>$10^{-6}$</td>
<td>$10^{-5}$</td>
</tr>
</tbody>
</table>

Given the parameters of our experimental setup, we have found out that the minimum acceptable visual quality of the decrypted image had $18 \times 18$ pixels per informative element (a letter of a text). The encryption of the text messages with a smaller information element is possible, but the decrypted image will be of poor quality and unreadable.

Furthermore, we have assessed the decrease of the resolution of the decrypted images compared with the resolution of the optical registration system without encryption. The purpose was to determine the identification threshold of decrypted messages given the parameters of the optical setup. For this purpose, we rescaled the registered (original) test images using the bi-cubic scaling. We noted that it is impossible to identify the text message with the number of pixels per informative element (a letter) of at least $7 \times 7$ pixels. This is consistent
with our previous results when the optically encrypted text can be decrypted and identified (i.e., the message is readable) when the size of an information element is 8 × 8 or more.

Therefore, the optical system without encryption provides identification of the decrypted images if the size of information element of 8 × 8 pixels, while the optical system with encryption - if the information element of 18 × 18 pixels. Given that, we can estimate the decrease in the resolution of about 2.3 times compared to the optical system without encryption.

Thus the experimental results allow saying that decrease in the resolution of the proposed optical encryption system is about 2-2.5 times compared with the optical system without coding. This leads to an NRMS error of the decrypted image from the original one of 0.40, which can be considered as satisfactory for the typical size of the optically encoded images and encryption PSF of a DOE.

6. CONCLUSIONS

The paper presents the concept and the experimental results on hybrid optical-digital encryption system. The encryption is performed optically and based on the “wavefront coding” paradigm. In the present optical setup, this is a convolution of the PSF of the phase-only DOE with the image of the input scene. The decryption is performed by digital deconvolution algorithms with the image of DOE’s PSF as a decryption key. In order to make the encryption system portable and inexpensive, we use consumer-grade digital SLR cameras. However, the use of such cameras requires post-processing to get images with linear response to light.

The text samples printed on a paper were optically encrypted in spatially incoherent laser and then digitally decrypted. Using one letter of the text (“information element”) as a measure of readability, we have estimated the NRMS error between the decrypted image and the original. For the text samples were the letters are big (font size 16-14 pt / the information element on the image is about 25 × 25 pixels), the NRMS error is 0.25, which corresponds to visually good quality of the decoded images. For the text samples were the letters are small (font size 12-10 pt / the information element on the image is about 20 × 20 pixels), the NRMS error is 0.30...0.38, which is satisfactory visual quality. We estimate the resolution deterioration in such an encryption system of 2-2.5 times compared with the same optical system without encryption. The NRMS error between the original and decrypted images in such case is less than 0.40 that is acceptable.

Summing up the above, we can say that the proposed hybrid optical-digital encryption system provides fast and secure optical encryption and easy-to-implement decryption with digital deconvolution algorithms. The experimental results presented in this paper show that the quality of the decrypted images is acceptable. Thus the proposed hybrid optical-digital encryption system can be considered as a reliable, portable, and inexpensive solution for the security needs.

REFERENCES


