Discover the recent advances in electronics research and fundamental nanoscience.

Nanotechnology has become the driving force behind breakthroughs in engineering, materials science, physics, chemistry, and biological sciences. In this compendium, we delve into a wide range of novel applications that highlight recent advances in electronics research and fundamental nanoscience. From surface analysis and defect detection to tailored optical functionality and transparent nanowire electrodes, this eBook covers key topics that will revolutionize the future of electronics.

To get your hands on this valuable resource and unleash the power of nanotechnology, simply download the eBook now. Stay ahead of the curve and embrace the future of electronics with nanoscience as your guide.
Multiplexing Optical Images for Steganography by Single Metasurfaces

Yue Cao, Lili Tang, Jiaqi Li, Chengkuo Lee,* and Zheng-Gao Dong*

Image steganography based on intelligent devices is one of the effective routes for safely and quickly transferring secret information. However, optical image steganography has attracted far less attention than digital one due to the state-of-the-art technology limitations of high-resolution optical imaging in integrated devices. Optical metasurfaces, composed of ultrathin sub-wavelength meta-atoms, are extensively considered for flat optical-imaging nano-components with high-resolutions as competitive candidates for next-generation miniaturized devices. Here, multiplex imaging metasurfaces composed of single nanorods are proposed under a detailed strategy to realize optical image steganography. The simulation and experimental results demonstrate that an optical steganographic metasurface can simultaneously transfer independent secret image information to two receivers with special keys, without raising suspicions for the general public under the cloak of a cover image. The proposed optical steganographic strategy by metasurfaces can arbitrarily distribute a continuous grayscale image together with a black-and-white image in separate channels, implying the distinguishing feature of high-density information capacity for integration and miniaturization in optical meta-devices.

1. Introduction

With the coming of the information age, people pay increasing attention to information security.[1] Steganography as an emerging technology branch of information security is of great significance for exploration,[2,3] which can hide secret information from the public in various ways such as images, videos, and audios.[4–6] As is known, image is one of the main sources for people to obtain and exchange information. Hence, image steganography is important to maintain information security.[7–9] The key technology of image steganography has been well-developed in the past decade, and its fundamental purpose is to securely transfer encrypted images on a public channel without raising suspicions.[10–12] However, existing methods of image steganography are generally in a digital route, and can only achieve a single channel, which means one sender transfers encrypted information to one receiver.[13] Therefore, it will be urgent to develop strategies for multiplexing imaging steganography, which is essential for multifunctional integration and miniaturization.

Metasurfaces, a class of artificial flat optical elements with feature cell size less than half wavelength, exhibit unprecedented abilities to manipulate the polarization, amplitude, and phase of incident light at the subwavelength level of the individual unit cell.[14–16] A variety of functionalities have been demonstrated such as flat metalenses,[17–20] holograms,[21–23] nanoprinting images,[24–26] and vortex generations.[27,28] In recent years, researchers have devoted more attention to multifunctional applications and integrated meta-devices.[29–32] Therefore, multifunctional metasurface may be introduced to the emerging field of optical image steganography, rather than the familiar digital-image steganography, which will address the issue of single-channel steganography,[33,34] so that a sender can transfer independent information to multiple receivers. In this multiplexing optical image steganography case, some secret information can be embedded into a media and extracted by multiple receivers with specialized keys.[23,35–37]

In this paper, we proposed a new strategy to generate multiplexing optical image steganography using a single metasurface, consisting of simple nanorods with different in-plane orientation angles. This strategy is to introduce optical image steganography into the design process of multifunctional metasurface to transfer multiplexing secret information to different receivers, where each independent secret information can be extracted by a corresponding key. Compared with existing image steganography, the proposed multiplexing steganography of optical images can simultaneously transfer different secret image information to respective receivers, meanwhile, a cover image is revealed to the general public. The simulation and experimental results were performed to show that the designed metasurface can hide two secret images under the disguise of
a cover image. The developed strategy to realize multiplexing optical image steganography by a single metasurface can break the mono-channel limitation of this technology and brings forward a single-metasurface perspective for multiplexing optical image steganography as a kind of integrated and miniaturized meta-devices.

2. Results and Discussion

The existing digital-image steganography method is shown in Figure 1a, which demonstrates that secret data is embedded into a given digital image for transfer to a receiver. Figure 1b is a framework of multiplexing optical image steganography analogous to the digital one, where concealed image information can be embedded into a single metasurface. Here, a grayscale image (secret information 1) and a quick response (QR) image (secret information 2) are used as steganographic information. Then, multiple receivers can extract the information with corresponding keys of different polarization states of the optical beam. However, the general public will be concealed by the cover optical image with uniform intensity if they have no keys. Figure 1c shows the schematic of multiplexing optical image steganography based on a single metasurface, with different linear polarizations of light as the keys. That is, under a normal illumination of the optical beam, the reflected beam can be visualized as three optical images, one is the cover image exhibited under white light for the public, while the other two are the concealed secret images extracted by lights with certain linear polarization angles $\theta$, which are defined as key 1 ($\theta = 0^\circ$) and key 2 ($\theta = 45^\circ$).

To embed two concealed images into a single metasurface, we propose an approach that can present multiplexing displays under different linearly-polarized illuminations at 900 nm. First, we designed a monolayer metasurface that can arbitrarily manipulate the reflected intensity by rotating the orientation angles of each unit cell with structural parameters shown in Figure 2a. To intuitively confirm the manipulation capacity of the designed metasurface, simulated reflectance spectra of periodic metasurfaces consisting of nanorods with different orientation angles are presented in Figure 2b, which demonstrates the relationship between the orientation angle of nanorod and reflection intensity.

Theoretically, when a linearly polarized beam with an intensity of $I_0$ passes through an optical polarizer and an anisotropic nanorod in turn, where the polarization direction of the polarizer is $\theta_p$ and the orientation angle of the nanorod is $\theta$, the intensity of output light can be expressed as

$$I = I_0 \left( A \cos^2(\alpha - \theta) + B \sin^2(\alpha - \theta) \right)$$

where $A$ and $B$ represent the complex reflection coefficients of nanorod corresponding to the polarization components along its long and short axes, respectively. The proposed nanorod can be regarded as an ideal polarizer according to resonance modes along with its long axis, which can arbitrarily manipulate the reflection by changing the orientation angle $\theta$ (Equation 1). So, for linearly $x$-polarized illumination, we can write $A = 1$ and $B = 0$, and thus

$$I = I_0 \cos^2(\alpha - \theta)$$

It verifies that the intensity of output light can be controlled by adjusting the difference between the orientation angle $\alpha$ and the polarization direction of polarizer $\theta$. This theoretical analysis is fully consistent with the simulation results in Figure 2b, demonstrating a feasible way of manipulating the intensity of output light by the orientation angle.

As shown in Equation (2), both the orientation angle and polarization angle of incidence (i.e., $\alpha$ and $\theta$, respectively) can be flexibly adjusted as per requests, which provides an additional degree of freedom to increase the imaging channels compared with the common imaging metasurface. Consequently, a multiplexing steganographic metasurface embedded with a grayscale image and a QR image can be successfully designed (Figure 3a), the details of choosing polarization channels are shown in Figure S1, Supporting Information, and the proposed strategy is described as follows. Due to the configuration of the unit cell, two nanorods that are symmetric with respect to the polarization direction of incidence have the same reflection intensity ($\theta_1 = \theta_2$), however, it becomes different if the polarization direction of incidence is rotated such that the symmetry is broken ($\theta_1 \neq \theta_2$). As is shown in Figure 3b, two pixels with the same gray level can choose two nanorods that are symmetric with respect to the $x$-direction of incident polarization. However, these two nanorods reflect opposite gray levels when the polarization direction is changed on conditions. It is worth noting that if the reflection intensity is larger than 0.5, the gray level is regarded as 1, otherwise, it is regarded as 0. Figure 3c is a flowchart for the steganographic metasurface, which in detail describes the design process. First, according to theoretical analysis and simulation results, two optimal polarization angles ($\theta_1$ and $\theta_2$) are chosen for a multiplexing metasurface. Then, the initial distributions of the orientation angles ($\alpha_1$) of image 1 are calculated, where each pixel of image 1 matches two orientation angles ($\alpha_1$ and $\pi - \alpha_1$). Next, the gray level of image 2 can be divided into two groups (i.e., bright and dark), corresponding to the reflection intensities $I_1$ of 1 and 0. Further, the final orientation angles are judged according to reflection intensity $I_2$. That is, if the intensity value of $I_2$ is 1, the corresponding final orientation angle ($\alpha$) is $\alpha_1$. On the contrary, the final orientation angle ($\alpha$) is $\pi - \alpha_1$. Finally, all orientation angles of the nanorod are obtained after judging operations cell by cell.

Accordingly, we design two different steganographic metasurfaces (Samples A and B) for a demonstration of the multiplexing optical image efficiency, and the simulation and experimental results are shown in Figure 4. Here, two continuous grayscale images of Einstein are recorded as the secret information 1 for receiver 1 with key 1 ($\theta_1 = 0^\circ$), while a QR image and a logo of Southeast University are chosen as the secret information 2 transferred to receiver 2 with key 2 ($\theta_2 = 45^\circ$), and two white images with uniform intensity are the cover images to confuse the general public, under the illumination of white light without the filter and polarizer. Figure 4a–c shows the simulation results of the multiplexing steganographic metasurface (Sample A), which can independently present three pictures, extracted by different illumination conditions. Figure 4d–f is the corresponding experimental results that are well consistent with the simulation results. Similarly, the simulation and experimental results for Sample B agree well with each other, as shown in Figures 4g–l.
respectively, indicating that the proposed approach is universally adaptable and can embed arbitrary grayscale images as secret information. It obviously reveals that all images extracted by the receivers have great clarity and high fidelity, which is beneficial for improving security and information capacity.

Figure 1. a) Existing strategy of the digital-image steganographic framework. b) The proposed strategy of multiplexing optical image steganographic framework in analog to digital steganography. A grayscale image and a QR image are chosen as the secret information embedded into a metasurface, while a cover image with uniform intensity is for the public. c) Schematic of the multiplexing optical image steganography, extracted by different polarizations of the reflected beam. When the metasurface is illuminated by white light, a uniform grayscale image can be observed, which is considered as the cover image for the general public. For extraction of the concealed secret image information, a bandpass filter and a polarizer can generate the key beam with a specific wavelength and linear polarization state. Here, the off-axis display of three reflected light beams is just for illustration of the design strategy and all three images are on the same axis in the actual optical imaging system. The images of Einstein appear with permission of the Albert Einstein Archives.
It should be noted that according to our design method and the discussions about Figure S2, Supporting Information, the proposed two-channel optical images for steganography are the upper limit of channels for this single metasurface. In order to adopt the QR image to store more secret information data, we have chosen a uniform blank intensity profile as a cover image.

Figure 2. a) Schematic of the unit cell with the Ag nanorod positioned on a silicon dioxide (SiO₂) substrate, which has dimensions of length \( L = 280 \) nm, width \( W = 135 \) nm, thickness \( T = 100 \) nm, and period of cell \( P = 420 \) nm. The orientation angle of the nanorod is \( \alpha \). b) Simulated reflection in dependence of orientation angle under \( x \)-polarized illumination.

Figure 3. a) Design principle of multiplexing steganography based on a single metasurface. For example, two pixels have the same gray level marked with purple boxes in secret information 1, but these two pixels have different gray levels (black and white) in secret information 2, we can choose two cells (cell 1 and cell 2) with different orientation angles \( (\alpha_1 \text{ and } \alpha_2) \), respectively. b) The selection principle of orientation angles of the multiplexing steganographic metasurface. Here, we set 0.5 as the threshold to distinguish the black (0) and white (1) gray levels. The first subscript of \( \theta \) represents the number of cells, and the second subscript is marked to distinguish two different polarization directions. c) Flowchart of designing the proposed steganographic metasurface. The images of Einstein appear with permission of the Albert Einstein Archives.
to hide the secret information because it will not occupy additional channels. Otherwise, only mono-channel steganography can be realized by scarifying one of the two concealed images to be the public image. Nevertheless, to avoid the possible disadvantage of a blank cover image which may raise suspicions, it is expected that we can design optical image steganography with a common cover image by complicated structural or multilayer metasurfaces. But up to now, an available method is not yet found to overcome it.

In addition, we present the simulation results of Sample A under illuminations with other linear polarization angles at 900 nm (see Figure S3, Supporting Information). The results demonstrate that the multiplexing steganographic metasurface has a high key precision to decode secret information.

Further, we explore the band response of optical image steganography, three narrow-bandpass filters were used to generate the pre-set illuminations at 850, 900, and 1064 nm. Figure 5 shows the experimental results of two concealed images under different wavelengths.

---

**Figure 4.** Simulation and experimental results of the multiplexing steganographic metasurface for samples A and B. The first and second rows present the secret information 1 and 2, which are transferred to different receivers with extraction key 1 \( (\theta_1 = 0^\circ) \) and key 2 \( (\theta_2 = 45^\circ) \), respectively. The third row shows the cover images for the general public without any key. The images of Einstein appear with permission of the Albert Einstein Archives.

**Figure 5.** Experimental results of multiplexing steganographic metasurface at wavelengths 850, 900, and 1064 nm. The images of Einstein appear with permission of the Albert Einstein Archives.
different wavelengths, exhibiting that the secret information images extracted by receivers will have the best definition only when the illumination is at a set wavelength of 900 nm, while for other neighboring wavelengths, there are certain degrees of distortion of the extracted information images. It demonstrates that the optical multiplexing steganographic metasurface needs a strict limit on the wavelength of the incident light, which also can be regarded as a kind of security factor to avoid the public to steal secret information.

3. Conclusion

We have demonstrated a multiplexing optical image steganographic metasurface that can record a continuous grayscale image and a monochrome image as two concealed secret information to be extracted by different receivers with given keys, under the cloak of a cover image. First, in analog to the well-known digital steganography, the strategy of multiplexing optical steganography was developed. Then, the metallic steganographic metasurface was designed, which consisted of single nanorods with different orientation angles to manipulate the pixelated distribution of reflection intensity arbitrarily. Further, we fabricated the proposed multiplexing optical image steganographic metasurfaces, to experimentally demonstrate that they could present high-resolution and high-fidelity images in independent channels with different keys of polarization and wavelength of light. Our work provides a simple solution to realize multiplexing optical image steganography, which would pave a potential way for information security, image display, high-density optical storage, and related fields.

4. Experimental Section

To obtain the optimum performance of the metasurface depending on the reflection intensity, the parameters (length, width, thickness, and period) of the nanorod were numerically swept by a computer simulation technology package, and accordingly fabricated multiplexing steganographic metasurfaces. In this experiment, all metasurfaces were fabricated on SiO2 substrates. The first step in fabricating a steganographic metasurface was to clean the substrate with acetone solution, ethyl alcohol solution, and deionized water, to efficiently decrease the influence of impurity. Following this, a uniform coating of polymethylmethacrylate was amorphously spin-coated onto the substrate, which was heated at 180 °C on a hot plate for 2 min. Then, the designed patterns were etched by an electron beam lithography. Finally, an amorphous Ag layer of 100 nm thickness was deposited by high-vacuum thermal evaporation, followed by a lift-off process in tepid acetone at 60 °C to remove the unnecessary Ag film. Figure 6 shows scanning electron microscopy images of Sample A. Significantly, all designed steganographic metasurfaces have 118 x 118 pixels, the overall size is about 50 x 50 µm, and the scale bar is 5 µm.

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

The authors acknowledge support from the National Natural Science Foundation of China (12174052, 11774053); The China Scholarship Council (Grant No. 202106090162).

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

metasurfaces, multiplexing imaging, steganography