Continuous development of security features is mandatory for the fight against forgery of valuable documents and products, the most notable example being banknotes. Such features demonstrate specific properties under certain stimuli such as fluorescent patterns glowing under ultraviolet light. These security features should also be hard to copy by unlicensed people and be interrogated by anyone using easily accessible tools. To this end, this Letter demonstrates the development of an ideal security feature enabled by the realization of modular metamaterials based on metal–dielectric–metal cavities that consist of two separate parts: metal nanoparticles on an elastomeric substrate and a bottom mirror coated with a thin dielectric. Patterns generated by creating nanometer-thick changes in the dielectric layer are invisible (encrypted) and can only be detected (decrypted) by sticking the elastomeric patch on. The observed optical effects such as visibility and colors can only be produced with the correct combination of materials and film thicknesses, making the proposed structures a strong alternative to compromised security features. © 2019 Optical Society of America

https://doi.org/10.1364/OL.44.004507

Optical security features generate visual effects that are hard to imitate aiming authentication of original products [1]. Such features are ubiquitous and on many products of intellectual property such as electronics, licensed merchandise, books, and valuable papers/documents. Banknotes use a number of optical security features some of which are fluorescent fibers embedded in paper glowing under ultraviolet light, watermarks appearing under certain illumination conditions, patterns changing colors with changing angle of view (iridescence), images created by infrared absorbing or reflecting prints [2]. The simultaneous use of these features improves the security of the product. As some of the features may be compromised over time, continuous development of new ones is a requirement to continue the anti-counterfeit efforts. Optical security features can also be designed for optical data encryption. Although authentication and optical data encryption are typically used interchangeably in the literature, there is a critical difference between these two domains of applications: the information must be completely invisible in the encrypted state and be decrypted only with the right key for optical data encryption. Although optical data encryption is less common than authentication, its popularity increases as its need is anticipated to be inevitable in the near future with the ever-increasing computing power [3].

Most of the recently developed optical security features address both authentication and data encryption functions and take advantage of the advancements in the microfabrication techniques. A variety of optical phenomena are used for these reports, including optical interference [4,5], plasmonics [6–12], photonic crystals [13–15], holograms [16,17], dielectric metasurfaces [18], luminescence [19], and Pauli blocking [20]. The encrypted patterns in these reports are created using optical or e-beam lithography [5–8,10,11,16–18], ultraviolet radiation [4,13], O₂ plasma [14], laser scanning [9], printing on paper [20], stamping [12,15], and stenciling [5]. The patterns are then decrypted (or encrypted, if they are decrypted as fabricated) by applying humidity [4,14], magnetic field [13], spectroscopic scanning [6], polarized laser light [9,16], exposure to O₂/H₂ gases [7,17], changing the refractive index of the medium [18], applying electrical signal [20], and observing the thermal image [5,10,11]. Despite these successful demonstrations, the adaptation of these techniques into practice is limited mainly due to the scaling issues associated with the low yield and the need for sophisticated equipment during microfabrication or decryption/encryption. A promising alternative is using metal–dielectric–metal optical cavities that eliminate the need for generating micro- or nanoscale patterns, and enable the use of the naked eye or cameras to detect the patterns that are created by simply changing the dielectric thickness. Such an approach has been previously used for static color printing [21]. To adapt the optical cavities for security applications, this Letter realizes dynamic (modular) optical cavities by transferring the top metal layer on a separate transparent elastomeric substrate (patch) and encrypting the data as nanometer-thick patterns on the dielectric [Fig. 1]. Ultrathin top metal layers dewet the surfaces and form nanoparticles [22] creating metamaterials when they are stuck on the bottom part of the cavity.
The novelty of this Letter is the realization of modular optical cavities using a scalable fabrication scheme and adapting them for convenient dynamic optical data encryption and authentication.

An optical cavity consists of a top absorber, e.g., a thin metal film, separated from a bottom mirror by a lossless dielectric layer. The optical response of such a cavity is determined by the optical properties and the thickness of each layer. For instance, an optical cavity consisting of 10 nm silver film as the absorber, 120 nm thick $\text{SiO}_2$ as the dielectric, and an optically thick (>80 nm) silver film as the mirror absorbs the red spectrum of the visible regime exhibiting blue surface color. A small increment in the dielectric thickness redshifts the reflection spectrum and creates a lighter blue surface color [Fig. 2(a)]. As a result, any pattern generated by changing the dielectric thickness is visible to the naked eye and cameras. Without the top absorber layer, however, the rest of the structure is an interference surface whose reflection spectrum is very similar to that of the bottom mirror [Fig. 2(b)], hiding (encrypting) the small change in the dielectric layer’s thickness. Decryption can be achieved by coating the absorber layer directly on the pattern. However, this method is inconvenient, as it requires access to a deposition tool, and it cannot be reversed. To enable convenient, dynamic, and reversible decryption, we demonstrate using a transparent elastomeric substrate such as a polydimethylsiloxane (PDMS) patch that is precoated with the absorber layer. The patch is then stuck on the pattern for decryption and removed for re-encryption [Fig. 1]. While our decision of using PDMS as the elastomeric substrate is based on our experience with the material, it has recently enabled other modular optical applications such as enhanced fluorescent emission using Au-nanoparticles-coated-PDMS [23] and upconversion amplification by embedding lanthanide-doped nanocrystals in PDMS [24].

The optical cavities in Figs. 1 and 2 are based on 10 nm top Ag layer and 120–130 nm $\text{SiO}_2$ that are chosen after visualizing the color space that is attained by varying the thicknesses of the Ag and the dielectric layers. For the static cavities, 10 nm top Ag layer produces shades of blue as the $\text{SiO}_2$ thickness varies between 100 and 160 nm [Fig. 3(a)]. For increasing Ag thickness, the surface colors are richer, but also fainter as the absorbance dip (resonance) sharpens [Fig. 3(b)]. Top-down scanning electron microscope (SEM) images of 10 nm Ag film show nanoparticle formation [Fig. 3(c)]. As a result, the optical response of the cavity with the percolating top silver film exhibits a wider and deeper resonance compared to a simple cavity consisting of continuous and flat layers. The measured optical response is matched by the numerical simulations when the percolating behavior of the top Ag film is accounted for.
The color space for the modular cavities is similar to that of the static ones for the top Ag thickness of 10 and 20 nm with slight shifts in the surface colors as a result of the refractive index of PDMS being larger than that of air [Fig. 4]. The SEM images of the silver films on PDMS exhibit similar behavior to those on SiO₂ surfaces explaining the similarity of the color spaces. However, the surface colors of the static and modular cavities for 30 nm Ag thickness do not match, possibly due to the damages the silver film accumulates during repetitive sticking and removal of the patch.

The color contrast for changing dielectric thickness is more crucial than the surface color for the proposed operation. Thus, the color contrasts for 10 nm thick patterns are tested by varying the thicknesses of the top Ag film and the SiO₂ layer. The results show clear color contrasts for the thickness range of 10–20 nm for Ag and 120–140 nm for SiO₂. Considering the observed contrasts and the robustness of the thin Ag films, the top Ag thickness is chosen as 10 nm for the following cases. While the pattern thickness for these cases is chosen as 10 nm as it is found sufficient for successful encryption and decryption, it is demonstrated that the patterns can be as thin as 2 nm to be successfully distinguished when decrypted.

The versatility of our approach is demonstrated using rigid and flexible substrates. Silicon wafers are the first choice as they are readily available in a lab environment and are suitable for any microfabrication process such as photolithography [Figs. 5(a) and 5(b)]. Most of the patterns are created using stenciling (shadow masking). The stencils are produced by laser cutting of 150 μm thick acetate sheets. While this method enables large-scale images, the resolution is limited with the laser-cutting process and the thickness of the stencil. An alternative is photolithography that is capable of producing high-resolution, large-area patterns. Figure 5(c) shows a decrypted QR code pattern created using photolithography. The QR code is completely invisible to the naked eye without the top Ag film. Thus, it is not suitable for optical data encryption, but can only be used for authentication.

The optical data encryption relies on invisibility of the patterns without the PDMS patch and a noticeable color contrast with the patch on. Therefore, there is a lower limit on the pattern thickness to successfully decrypt the patterns and an upper limit to properly encrypt them. The upper limit strongly depends on the reflectance of the mirror layer and can be larger for higher reflectance. For instance, a perfect mirror with 100% reflectance would demonstrate the same performance with a lossless dielectric layer of any thickness on it. Thus, the patterns can have any thickness and still be invisible to the naked eye. For an actual metal mirror, however, the reflectance is lower than 100% and with a dielectric layer on top of the mirror, absorption of the incident light further increases as a result of enhanced interaction of the light and the metal. In this case, a small change in the dielectric thickness can shift the reflection spectrum significantly enough to be noticed by the naked eye.

The code is revealed by sticking the Ag-coated PDMS patch on and can be scanned after enhancing the contrast of the image.

As our approach involves blanket deposition of thin films and stenciling for creating patterns, it can be adapted for any substrate, including the flexible ones such as plastic sheets and aluminum foils [Figs. 5(d) and 5(f)]. The use of metal foils is especially promising, as they can provide both mechanical support and high reflectance acting as the bottom mirror. The use of flexible substrates helps to bring down the fabrication cost and, more importantly, enables optical security features on almost any surface that can hold a metal layer such as banknotes. Creating a multicolor pattern is also possible by defining the pattern using multiple thicknesses [Figs. 5(g) and 5(h)]. In this case, however, most of the pattern can be detected by the naked eye without the top Ag film. Thus, it is not suitable for optical data encryption, but can only be used for authentication.

The optical data encryption relies on invisibility of the patterns without the PDMS patch and a noticeable color contrast with the patch on. Therefore, there is a lower limit on the pattern thickness to successfully decrypt the patterns and an upper limit to properly encrypt them. The upper limit strongly depends on the reflectance of the mirror layer and can be larger for higher reflectance. For instance, a perfect mirror with 100% reflectance would demonstrate the same performance with a lossless dielectric layer of any thickness on it. Thus, the patterns can have any thickness and still be invisible to the naked eye. For an actual metal mirror, however, the reflectance is lower than 100% and with a dielectric layer on top of the mirror, absorption of the incident light further increases as a result of enhanced interaction of the light and the metal. In this case, a small change in the dielectric thickness can shift the reflection spectrum significantly enough to be noticed by the naked eye.

**Fig. 4.** Photograph of the modular optical cavities formed by sticking 10, 20, and 30 nm Ag-coated PDMS patches. Scale bars: 1 cm.

**Fig. 5.** Examples using various substrates and fabrication methods. (a)–(b) Hiding and revealing the pattern in a cavity on a Si substrate. The base SiO₂ thickness is 120 nm. See Visualization 1 for dynamic decryption and re-encryption. (c) Revealed QR code pattern. The base SiO₂ thickness is 135 nm. Visualization 2 shows dynamic decryption and re-encryption. The use of (d) plastic and (e)–(f) Al foil as flexible substrates. Al foil is also coated with a 120 nm Ag mirror. Thus, the foil only serves as a mechanical support. (g)–(h) A flower pattern generated by changing the SiO₂ thickness from 90 nm (for the background) to 160 nm (for the center) by 10 nm increments in a clockwise direction. Scale bars: 1 cm.
For instance, while 10 nm thickness difference in the SiO₂ dielectric layer is completely invisible on a high-reflectance Ag layer; it can be noticed by the naked eye at certain angles of view and lighting conditions for a Ag layer with lower reflectance. Therefore, for proper encryption, either high-reflectance metal mirrors should be used or patterns should be ultrathin at nanometer-thick changes in the dielectric layer are encrypted by repeatedly sticking and removing the PDMS patch. Neither the PDMS patch nor the bottom part of the cavity shows any deterioration optically or mechanically after 200 cycles. However, it is observed that dust particles are captured between the patch and the SiO₂ surface. The accumulation of such undesired particles may adversely affect the optical performance during the decryption operation, especially for patterns with high resolution. This limitation can be mitigated by keeping the surfaces clean at all times. Another limitation of the method is the degradation of the top metal layer over time due to exposure to air. Possible solutions include using more resilient materials, e.g., Au, coating the metal layer with a thin barrier layer, and using metals that grow native oxide self-limiting the degradation process [22].

In summary, this Letter demonstrates the realization of modular optical cavities consisting of thin Ag-coated PDMS patches and SiO₂-coated bottom mirrors. Patterns defined as nanometer-thick changes in the dielectric layer are encrypted without the PDMS patch and decrypted when the patch is stuck on the pattern, defining a new optical security modality. The proposed method can be employed for optical data encryption, as well as security (authentication) features aiming at anti-counterfeit applications.

**Funding.** Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (117E203).

**REFERENCES**