Optical Engineering

SPIEDigitalLibrary.org/oe

Optical security device providing fingerprint and designed pattern indicator using fingerprint texture in liquid crystal

Keizo Nakayama
Junji Ohtsubo

SPIE

Optical security device providing fingerprint and designed pattern indicator using fingerprint texture in liquid crystal

Keizo Nakayama[a] **and Junji Ohtsubo**[b]
[a]Kinki University, Department of Electric and Electronic Engineering, Faculty of Science and Engineering, 3-4-1 Kowakae, Higashi-Osaka, Osaka 577-8502, Japan
[b]Shizuoka University, Department of Systems Engineering, Faculty of Engineering, 3-5-1 Johoku, Naka-ku, Hamamatsu, Shizuoka 432-8561, Japan
E-mail: keizo@ele.kindai.ac.jp

Abstract. An optical security device providing the function of a fingerprint for authentication along with a designed pattern storage function has been proposed. The proposed device uses the random fingerprint texture in the chiral nematic phase of an ultraviolet-curable liquid crystal. Using photopolymerization along with a mask of the designed pattern, a unique pattern can be fixed in the shape of the designed pattern. The random patterns can be used as a fingerprint for such devices. This proposed device has the potential to be an optical security device and an authenticity or information indicator for the user. [DOI: 10.1117/1.OE.51.4.040506]

Subject terms: security device; random feature; identification information; fingerprint; optical texture; liquid crystal.

Paper 111598L received Dec. 20, 2011; revised manuscript received Feb. 25, 2012; accepted for publication Mar. 6, 2012; published online Apr. 20, 2012.

Smart cards or chip cards with an embedded integrated circuit (IC) have been widely used to enhance security. Natural randomness, i.e., some uncontrollable variations in features have been extensively researched aside from digital technology, such as ICs. These features are difficult to tamper with or copy because of their random nature. Although many security devices have been proposed based on such random features, some devices that are relevant to optical technology will be discussed here. Two parallax images of a three-dimensional random arrangement of polymer fibers in nonwoven fabric embedded in a product have been proposed as a fingerprint (unique identification information).[1] Other devices researched for the same purpose include a transparent inhomogeneous medium[2,3] and a polymer light-emitting device,[4] where the speckle patterns of the former and the inhomogeneous emission patterns of the latter are random. Information that can be optically detected from the rough surface of the product itself has also been studied.[5,6]

Various optical textures that reflect the nonuniformity of the molecular orientation can be observed using a polarizing microscope for a combination of liquid crystal phases and glass surface conditions.[7] A random stripe pattern in the chiral nematic (N^*) or cholesteric phases in liquid crystal materials can be obtained in a cell following homeotropic surface treatment. This is because the N^* phase has a helical molecular orientation structure, and the helix axis is parallel to the substrates in the homeotropic cell. When the helix axis is not controlled, i.e., it is random in the plane of the substrates, the stripe texture is complex and looks like human fingerprints; these stripe textures are thus called fingerprint textures.

With consideration of the above, we have proposed the application of a random fingerprint texture pattern in a UV-curable liquid crystal for an index to distinguish individual products.[8] In this paper, we report the high randomness of the fingerprint texture in the N^* phase by using normalized cross-correlation. It was also demonstrated that the texture of this polymerized fingerprint was stable to over 105°C.

In this letter, we propose an optical security device that has the function of storing a designed pattern as well as the function of providing a fingerprint for authentication by using a fingerprint texture in the N^* phase of a UV-curable liquid crystal. The fabrication process of this device is not complicated because the photopolymerization technique is used.

The liquid crystal mixture used in this study was a UV-curable liquid crystal (UCL-001-K1, DIC Corp., Tokyo, Japan), doped with a chiral dopant (S-811, Merck Ltd., Tokyo, Japan) at 1.8 wt% concentration. This mixture exhibited an isotropic (Iso.)-N^* phase sequence, and the phase transition temperature T_{NI} from the Iso. phase to the N^* phase was 40°C. We determined the 1.8 wt% concentration that caused the appropriate fingerprint texture at the N^* phase experimentally.[8] The gap between the two substrates of the sandwich cell used (E.H.C. Co. Ltd., Tokyo, Japan) was 10 μm, and the substrate surfaces were treated to produce homeotropic alignment. To avoid the effects of flow alignment, the liquid crystal mixture was filled into the cells by capillary action at a temperature greater than T_{NI}. The photopolymerization reaction was carried out at UV intensity of 24 $\mathrm{mW/cm^2}$ for 30 s using a UV light source (ELC-410, Electro-Lite Corp., Danbury, Connecticut, USA).

To fabricate a device that was written with a designed pattern, the photopolymerization was performed through a patterned mask. The fabrication process consisted of the following steps. The temperature of the cell filled with the mixture was kept below T_{NI}, allowing the mixture to exhibit the complex fingerprint texture. Then, part of the cell was irradiated with UV light through the mask; only the mixture in the irradiated areas was photopolymerized, and the fingerprint texture was fixed. Next, the cell temperature was increased to above T_{NI}. The mixture in the nonirradiated areas then changed phase from N^* to Iso.; the fixed molecular orientation in the irradiated areas remained unchanged. Under these conditions, the whole area of the cell was irradiated, and the Iso. phase areas were polymerized. After these steps, the whole of the cell was polymerized to give the molecular orientation permanence. The polymerized N^* orientation (fingerprint texture) causes light scattering and optical anisotropy. On the other hand, ideally, the polymerized Iso. orientation (no texture) would cause no light scattering and no optical anisotropy.

We fabricated a device storing the pattern of a "6." This polymerized device actually was stable at 150°C for 30 min. This result indicates that the device has a sufficient heat

0091-3286/2012/$25.00 © 2012 SPIE

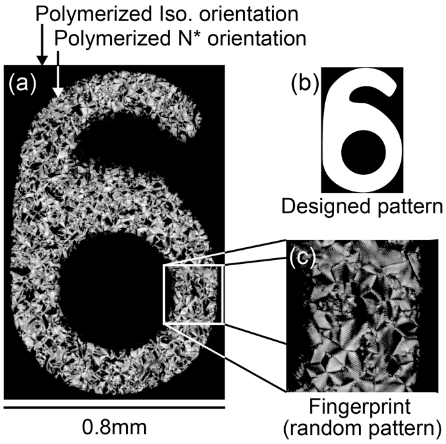

Fig. 1 Schematic of the proposed optical security device, providing both the designed pattern and the fingerprint: (a) polarizing microphotograph of the device; (b) the designed pattern stored in this device; and (c) the fingerprint or unique identification pattern.

resistance, since typical products, which need a security device, will be used at less than 150°C. Figure 1(a) shows a micrograph of the device taken by transmitted polarization observation (ECLIPSE E600 POL, Nikon Corp., Tokyo, Japan). This photograph shows the bright region of the polymerized N^* orientation and the dark region of the polymerized Iso. orientation. It is also noted that this device stores two kinds of information, as shown in Fig. 1(b) and 1(c).

First, this device stores the artificial information of the number six shown in Fig. 1(b). Using other masks with different desired patterns, devices with different patterns are simple to make. Also, the information can be made visible to the naked eye without the use of polarizers because strong light scattering comes only from the polymerized fingerprint texture in a specific arrangement of a light source, the device, and the viewer's eye line. Figure 2 shows a photograph of the device taken with a digital camera without polarizers against a black background. The pattern of a "6" was clearly visible because of strong scattering from the polymerized fingerprint texture alone, although the area of the polymerized Iso. orientation had some hazy parts. This result shows that this device can be used for the purpose of identification or as a simple information indicator for the user.

Second, the device can provide the fingerprint to identify itself. The bright region in Fig. 1(a) was made of the random fingerprint texture shown in Fig. 1(c). Even if many devices are made using the same mask and through an identical process, the fingerprint texture patterns for each device

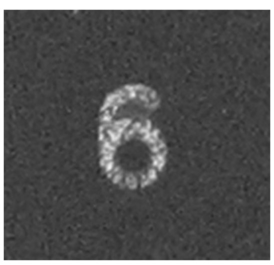

Fig. 2 Photograph of the device taken using a digital camera without polarizers.

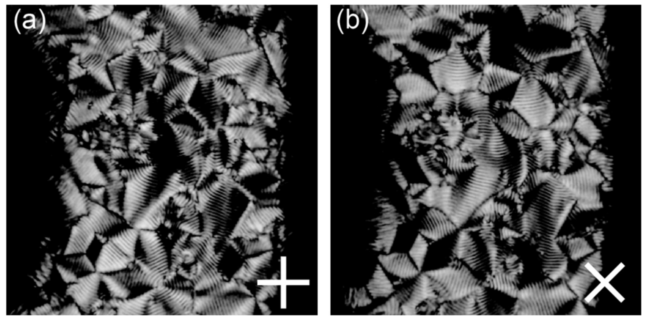

Fig. 3 Polarizing microphotographs taken in the same area of the same device under two different crossed polarizer configurations. The crosses represent the directions of the crossed polarizers.

cannot coincide because of the high randomness. These patterns can therefore be used as a fingerprint for each device. Consequently, these polymerized liquid crystal devices can act as security devices, providing the identification information for any individual product embedded with this security device. The multiplexing of the polarization information can also improve the level of security. Figure 3(a) and 3(b) are polarizing microphotographs taken in the same region of the same device; nevertheless, there are differences in optical intensity between the two photographs. This is because the angles of the crossed polarizers used in each photograph were different, and the optical intensity under polarizing observation depends on the configuration of the molecular orientations and the polarizers. Devices counterfeited on the basis of microphotography and microprinting technologies, which control the color and density of films, but not the anisotropy, cannot pass an authentication procedure using images taken using the different crossed polarizer configurations.

Finally, we outline a basic security system using the proposed security devices, assuming that the products with important authenticity are ID cards, as shown in Fig. 4. The proposed device is embedded in every ID card. Prior to the distribution of these ID cards, unique keys, which are simply polarization images detected optically from the embedded proposed device or some information generated from these images, are enrolled with an identification number in a database in an authentication server. When

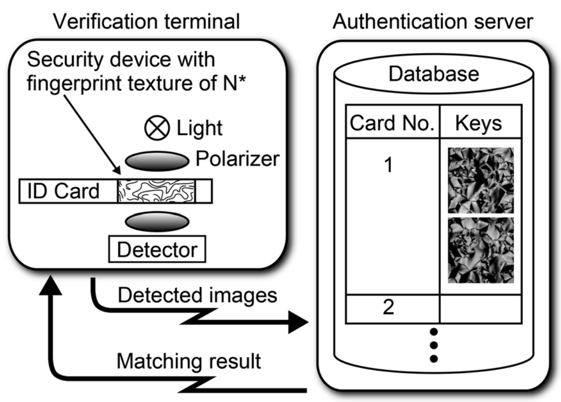

Fig. 4 Schematic diagram of a basic security system using the proposed devices.

the ID card is to be used, the polarization images detected directly from the ID card at a verification terminal must then be matched to the keys stored in the database before the use of the ID card is accepted. Because the proposed security device has a lot of information, such as a random pattern, polarization information, and a designed pattern, we can develop multiple matching algorithms to meet the demands on performance and security level.

In conclusion, we have proposed an optical security device having both the function of a fingerprint for authenticity and the function of storage for a designed pattern using the fingerprint texture in the N^* phase. An identical fabrication process enables each device to have unique fingerprint texture patterns that can be used as a fingerprint for products because of the randomness of the fingerprint texture. Multiplexing of the polarizing information can make counterfeiting difficult. This device can also store an artificially designed pattern as a partial fingerprint texture, and this pattern is visible to the naked eye without using polarizers. Accordingly, this proposed device has the potential to be used as an optical security device and as an authenticity or information indicator for the end user.

References

1. R. L. van Renesse, "3DAS: a 3-dimensional-structure authentication system," *Proceedings of European Convention on Security and Detection*, Institution of Electrical Engineers, London, pp. 45–49 (1995).
2. R. Pappu et al., "Physical one-way functions," *Science* **297**(5589), 2026–2030 (2002).
3. O. Matoba, T. Sawasaki, and K. Nitta, "Optical authentication method using a three-dimensional phase object with various wavelength readouts," *Appl. Opt.* **47**(24), 4400–4404 (2008).
4. K. Tada and M. Onoda, "Polymer light-emitting devices for artificial fingerprints," *Jpn. J. Appl. Phys. Part 2* **42**(9A/B), L1093–L1095 (2003).
5. T. Haist and H. J. Tiziani, "Optical detection of random features for high security applications," *Opt. Comm.* **147**(1–3), 173–179 (1998).
6. J. D. R. Buchanan, "'Fingerprinting' documents and packaging," *Nature* **436**(7050), 475 (2005).
7. Ingo Dierking, *Textures of Liquid Crystals*, Wiley-VCH, Weinheim (2003).
8. K. Nakayama and J. Ohtsubo, "Application of random texture in cholesteric liquid crystal for security devices," *Mol. Cryst. Liq. Cryst.* **516**(1), 253–259 (2010).