Optical spectrum fingerprint: a novel application of optics as an encryption-decryption technique

Gao, Andrew, Zhang, Bojun, Cao, Wenhao

Andrew Gao, Bojun Zhang, Wenhao Cao, "Optical spectrum fingerprint: a novel application of optics as an encryption-decryption technique," Proc. SPIE 11682, Optical Components and Materials XVIII, 116820B (5 March 2021); doi: 10.1117/12.2578643

SPIE.

Event: SPIE OPTO, 2021, Online Only

Optical spectrum fingerprint: a novel application of optics as an encryption-decryption technique

Andrew Gao, Bojun Zhang, Wenhao Cao
Silicon Valley Optics Technology

ABSTRACT

Various optical phenomena and techniques have been used to encrypt sensitive data and detect counterfeit objects. When two multilayer dielectric films of different indices are deposited in an alternating pattern on a glass substrate to form an optical filter, the transmission of this filter presents an optical spectrum. Because of the two materials' different indices, layer sequences, and number of layers, the spectrum of any one of these filters is unique and exclusive. The spectrum and corresponding multilayer structure, therefore, can be considered a spectrum "fingerprint" and can be used to encrypt confidential information. One can design a multilayer sequenced layer structure as an encryption code. Knowing the spectrum of this code, they can also design a decryption filter to analyze the code spectrum and access the information embedded in the encrypted filter. High and low index materials Ta2O5 and SiO2 were used to fabricate multilayer film stacks with around 5 to 10 high-low pairs. The spectrum has multiple peaks in the visible wavelength range and is designed such that the spectrum appears colorless. A decryption multilayer film would block all but one of the peaks, the transmission of which would reveal the color. In this study, we present how we can design an encryption and decryption spectrum, how one can use these spectrum "fingerprints" to store confidential information and, when necessary, access said information by placing a decryption filter above the encryption filter.

Keywords: spectrum fingerprint, spectra encryption and decryption, optical anti-counterfeit application, SiO2, Ta2O5 multilayer filter application

1. INTRODUCTION

Within Silicon Valley Optics Technology, Inc.'s optical coating R&D group, a project was initiated to study optical spectra coding and decoding for the purpose of developing a commercial optical encryption application for highly important products affected by counterfeit. Past studies have repeatedly shown hundreds of billions of dollars in losses annually due to counterfeit. The US Department of Justice estimates $10 billion worth of bad checks are passed every year. According to the FBI, annual check fraud in the United States is estimated to total $15 billion. In all, over 5% of world trade is counterfeit, and the global counterfeit market was estimated to be worth around 1.82 trillion USD as of 2020 [1]. As a result of these issues, there is a large market for novel anti-counterfeit technology. Products including passports, driver licenses, and birth certificates all require anti-counterfeit technology for protection. Current anti-counterfeit technologies on the market include watermarks, holograms, pigment printing, and optical variable printing among others. However, these technologies have many shortfalls. For instance, holograms account for 39% of the anti-counterfeit market. Yet, within 24 hours, counterfeit holograms for pharmaceutical products appear on the streets of Asia, prompting a new, harder-to-counterfeit substitute [2]. It takes the US Department of Treasury and Bureau of Engraving and Printing anywhere from 2-6 years to redesign American currency notes, allowing many counterfeiters ample time to develop fakes [3]. Fundamentally, current anti-counterfeit technologies are easy to forge, cumbersome in design, inaccessible without special instruments, or require special training to use [4,5,6]. To solve these issues, we propose a secure, easy-to-use, inexpensive, and versatile novel anti-counterfeit technology utilizing optical spectra coding and decoding.

Optical Components and Materials XVIII, edited by Shibin Jiang, Michel J. F. Digonnet,
Proc. of SPIE Vol. 11682, 116820B · © 2021 SPIE · CCC code: 0277-786X/21/$21
doi: 10.1117/12.2578643

The most common anti-counterfeit technology used for paper currency is optical particle powder prints that utilize the light reflection of the optical particles. In using this anti-counterfeit method, turning or rotating a banknote would change its color from dark yellow to green. Laser image printing also gives a similar result that distinguishes counterfeit labeling from authentic. However, we propose an even more secure approach which we call doubly-secured anti-counterfeiting using optical spectrum coding and decoding. We utilize the concept of multilayer interference to fabricate a unique, exclusive spectrum. Firstly, when the viewing angle is changed and the light path of the multilayer changes, the spectrum shifts so that the color of the multilayer varies. This is one phenomenon we utilize in our anti-counterfeit methodology. Secondly, we can build these spectra with multiple transmission peaks. When viewing this multi-transmission peak multilayer film at the right angle, it appears colorless. However, if we design and fabricate another multilayer interference film/filter that has shifted transmission peaks and place it on top of the coding spectrum filter, the decoding filter eliminates some of the transmission peaks of the coding filter. As a net effect, the leftover single transmission peak results in a pure color that is visible to the human eye. This is the second part to our doubly-secured anti-counterfeit methodology.

2. SPECTRA DESIGN AND EXPERIMENTAL

Both TFCalc and FilmStar design software were used in this project. Sample preparation was done using 2mm square BK-7 glass sheets. Substrate samples were polished in-house in our optics fabrication production line, and ultrasonic washed and alcohol wiped in our production cleaning line.

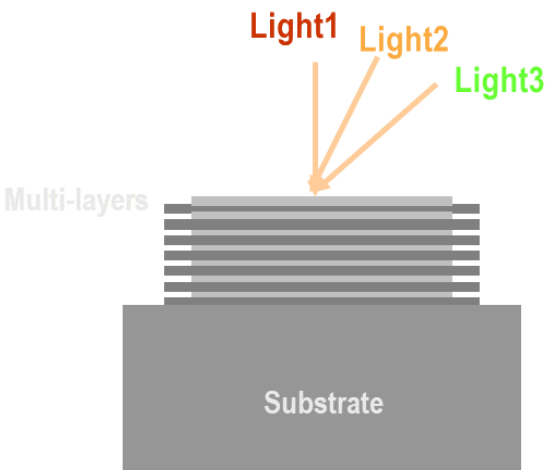

Fig. 1A

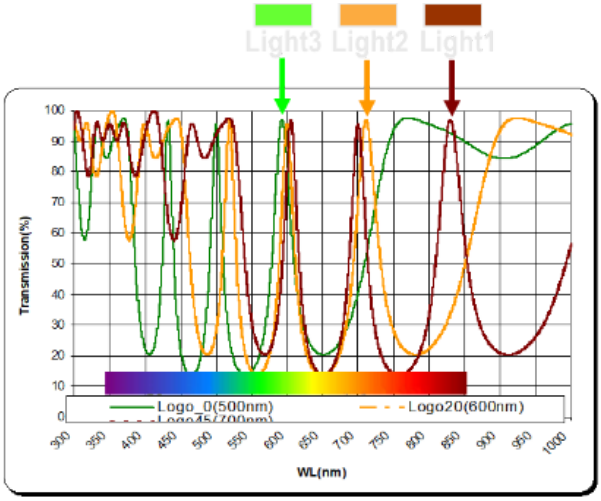

Fig. 1B

Figure 1A is a simple representation of how this multilayer interference film stack is designed and fabricated. It uses BK-7 as the substrate and has two index multilayer film stacks deposited on top. In this image, the three different arrows labeled Light1, Light2, and Light3 represent light striking the film stack from different viewing angles. The corresponding spectra of these three angles of incidence is shown and labeled in Figure 1B. Viewing the film stack from the normal, the perpendicular light path is shorter compared to the light path when viewing the film stack at an angle. Relative to the normal, a larger angle would result in a longer light path. This increase shifts the transmission peak of the spectra. Thus, when viewed by human eyes, the color of the film stack changes [7,8]. We used this phenomenon in the first part of the anti-counterfeit project.

3. FABRICATION AND RESULT

The machine used for filter fabrication was a Veeco Spector optical coating system. Measurements were done using Shimadzu and Agilent (Cary) spectrophotometers. Based on the level of encryption needed, the key spectrum filters may be fabricated using multilayers ranging anywhere from 4 to 100 HL pairs and the coating time ranging from 2 to 24 hours for both encryption and decryption spectra filter samples. A typical filter sample has 12 HL pairs.

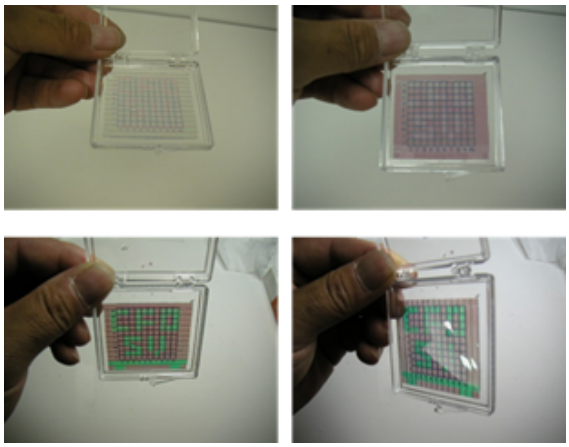

Fig. 2

Fig. 2 is a physical sample of the fabricated multilayer film stack design. The logo spectrum and background spectrum were designed and fabricated with the masking methodology, making the stack appear colorless from a normal viewing angle. In these two samples, one can observe that when viewing the film from the normal, nothing can be seen. However, changing the viewing angle, the transmission peak of the logo shifts while the transmission peak of the background remains unaffected. As a result, the logo color starts to appear when changing the viewing angle of the film stack. We can also build these spectra with multiple transmission peaks. When we view this multiple transmission peak multilayer film at the right angle, it appears colorless. To reveal this color, we can design and fabricate another multilayer interference decode film/filter that has shifted transmission peaks. Placing this decoding filter on top of the coding spectrum filter, the decoding filter eliminates some transmission speaks of the coding filter. As a net effect, the leftover single transmission peak is a pure color which can be easily perceived by the human eye [9,10,11]. This is the second component to the anti-counterfeit application, making it a doubly-secured anti-counterfeit methodology.

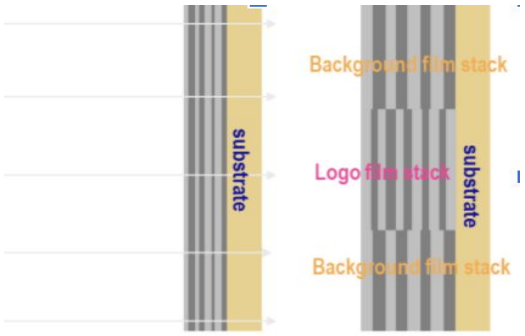

Fig. 3 Code over decode

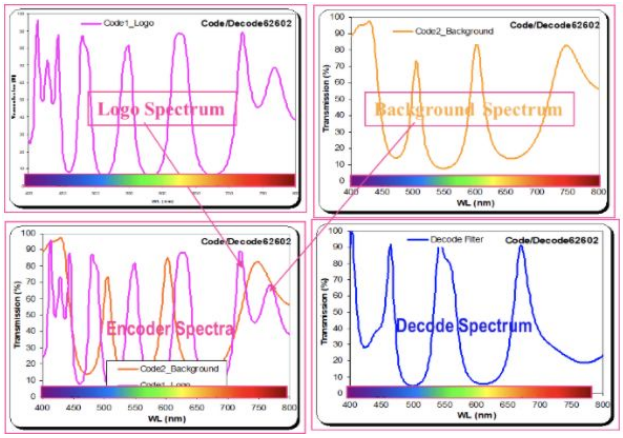

Fig. 4A (top left), B (top right), C (bot. left), D (bot. right)

Figure 3 shows a set of code and decode filters together which is the second part of this anti-counterfeit application. In the figure, a specially designed and fabricated decode filter lies on top of the code filter that was also designed and fabricated with masking methodology. The purpose of laying the decode filter on top of the code filter is to eliminate certain transmission peaks in the code filter spectrum which then changes the overall appearance. To illustrate this more clearly, Figure 4A shows the code (logo) spectrum; 4B shows the background spectrum; 4C shows the code and background spectra combined; 4D shows the decode spectrum. In the fabrication of the code embedded with the background, we used masking method.

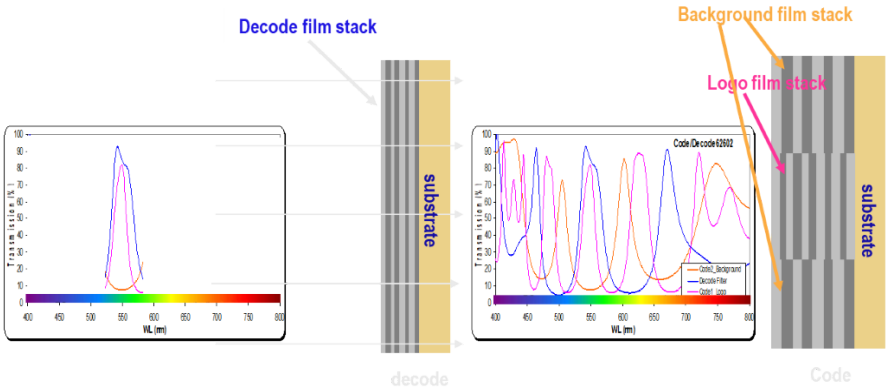

Fig. 5B Fig. 5A

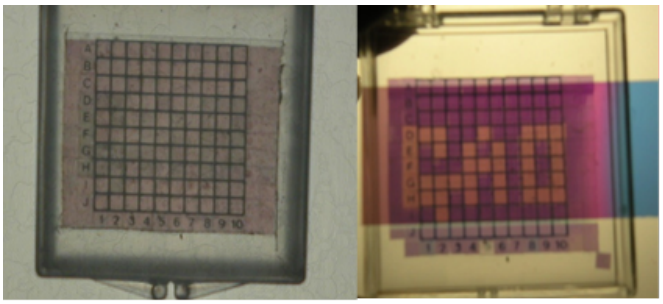

Fig. 6A Fig. 6B

Fig. 5A shows how this spectrum code and decode works. One can see from Fig. 4C that the combined code and background spectra is filtered by the decode spectrum. The decode spectrum eliminates two transmission peaks, one on the left and one on the right of the code transmission peak. The center peak of the code spectrum which is in the green color region remains unchanged. The net result is the leftover spectrum shown in Figure 5B, the color of which now appears visible to the human eye. Figure 6A and B are two examples of this decode filter laying on top of the code filter.

4. DISCUSSION

As previously mentioned, current anti-counterfeit technology has four common downfalls: they are easy to forge, cumbersome in design, inaccessible without special instruments, or require special training to use. Our key spectrum filters address these issues directly. Due to the high barriers to entry for design and fabrication of thin film filters, our code spectrum filters are highly secure and extremely hard to counterfeit [12]. No special training is needed to verify the

integrity of the product the code filters are used for. Anyone can simply lay the key filter on top of the lock filter or change their viewing angle. No special tools or instruments are necessary in order to use these filters, making it an extremely versatile, portable, and easy-to-use anti-counterfeit technology. Compared to other anti-counterfeit devices, our code and decode filters are also doubly-encrypted. One can either change their viewing angle by adjusting the filter itself or place the decode filter on top of the code filter to verify the integrity of the entity.

We see many real-life applications for this technology. As a measure of preventing counterfeit, various countries across the world have currency with transparent plastic windows designed into their banknotes. These plastic windows serve the same function as the key spectrum filter. However, whereas transparent plastic windows are easier to counterfeit and nonunique, the key spectrum filter is much harder to forge and each filter can be designed uniquely. Other applications include identification documents, such as passports, personal IDs, university diplomas, and driver licenses which all use optically variable ink—a less secure anti-counterfeiting method compared to code and decode filters [13,14]. Expensive consumer goods, including alcoholic beverages, branded apparel, and others, are other products that have promising potential for the application of our encryption-decryption spectrum filters.

5. CONCLUSION

In conclusion, our proposed novel anti-counterfeiting technology works as intended. After fabricating both the code and decode spectrum filters, placing the decode filter on top of the code filter successfully reveals the hidden pattern and thus serves as a viable anti-counterfeit technology. Although the code and decode spectrum filters have a wide variety of applications, physical wear and tear or damage to the code filter's thin film may make it more difficult to use. Durability is a serious concern for products which are expected to be held for long durations of time or handled roughly, such as expensive liquors or banknotes of small denominations. Another potential issue we foresee is single-unit costs. Since our per-unit production costs are inversely proportional to the number of filters produced, servicing a single highly unique order such as an expensive piece of artwork would be extremely expensive to produce. Despite this, our optical encryption-decryption filters hold numerous advantages compared to other anti-counterfeit technologies. In massive quantities, the per-unit production cost is very low. The code and decode filter technology is easy-to-use and has no environment limitation [15, 16]. The filters are also extremely difficult or near impossible to forge.

REFERENCES

[1] *Global Brand Counterfeiting Report, 2018: An indepth report on the size, modes, routes & issues underlying counterfeiting both through physical as well as online mediums* (Report No. 4438394). Research and Markets. https://www.researchandmarkets.com/research/hzjb9c/global_brand

[2] *Digital Holography Market by Offering (Hardware and Software) Application (Microscopy, Holographic Display, Holographic Telepresence), Vertical (Commercial, Medical, Automotive), Technique, Process, Region – Global Forecast to 2024* (Report No. 3760). Markets and Markets. https://www.marketsandmarkets.com/Market-Reports/digital-holography-market-136623896.html

[3] U.S. Department of Treasury Bureau of Engraving and Printing. Washington D.C., https://www.moneyfactory.gov/uscurrency.html

[4] Phillips, R., Bonkowski, R., Higgins, P., Markantes, C. (2007). *Optically variable security devices* (U.S. Patent No. 7224528). U.S. Patent and Trademark Office.

[5] Murashima, K., Shibata, T., Inoue, A. (2003). *Optical component, optical encoder, optical decoder, and optical communication system* (U.S. Patent No. 10/228265). U.S. Patent and Trademark Office.

[6] Sailor, M., Meade, S. (2015). *Optically encoded particles through porosity variation* (U.S. Patent No. 9181634). U.S. Patent and Trademark Office.
[7] Sailor, M., Schmedake, C., Link, J. (2014). *Optically encoded particles* (U.S. Patent No. 8765484). U.S. Patent and Trademark Office.
[8] Sailor, M., Meade, S. (2012). *Method for forming optically encoded thin films and particles with grey scale spectra* (U.S. Patent No. 8308066). U.S. Patent and Trademark Office.
[9] Yureschko-Suhan, N. (1998). *Playable optical picture disc* (U.S. Patent No. 5792538). U.S. Patent and Trademark Office.
[10] Pham, H., Gourevich, I., Oh, J., Jonkman, J. and Kumacheva, E. (2004), *A Multidye Nanostructured Material for Optical Data Storage and Security Data Encryption*. Adv. Mater., 16: 516-520.
[11] Artur Carnicer and Bahram Javidi, "Optical security and authentication using nanoscale and thin-film structures," Adv. Opt. Photon. 9, 218-256 (2017)
[12] Sencer, A., Gokhan, B. (2020). *Optical encryption and decryption structure with thin film surface coloring* (WIPO Patent No.112064A1). World Intellectual Property Organization.
[13] Gokhan Bakan, Sencer Ayas, Murat Serhatlioglu, Aykutlu Dana, and Caglar Elbuken, "Reversible decryption of covert nanometer-thick patterns in modular metamaterials," Opt. Lett. 44, 4507-4510 (2019)
[14] Sailor, M., Schmedake, T., Cunin, F., Link, J. (2015). *Manufactured product with optically encoded particle tag and ID method* (U.S. Patent No. 8765484). U.S. Patent and Trademark Office.
[15] Hoshino, H., Takeuchi, I., Sakauchi, T. (2015). *Identification medium, article equipped with identification medium* (European Patent No. 05819863.1). European Patent Office
[16] Basset, G., Gallinet, B., Dumpelmann, L., Luu-Dinh, A., Sauvage-Vincent, J., Schnieper, M. (2015). *Optical security component with plasmon effect and method for manufacturing such a component* (European Patent No. 025277A1). European Patent Office.