**Fingerprinting light emitting diodes using spectrometer**

A. Toh\(^{a}\), L. Yang, K. Sakiyama and T. Sugawara

Fingerprinting refers to a class of techniques to distinguish products using their unique features originated during production. Fingerprinting has a wide range of applications including supply-chain integrity and device authentication. The authors propose the first fingerprinting technique of light-emitting diode (LED), which is pervasively used in electronics products. The key idea is to use spectral features of LEDs obtained by a spectrometer. Combined with a machine-learning classifier, the proposed method successfully distinguishes ten individual LED samples from the same lot at 99% accuracy.

**Introduction:** Fingerprinting refers to a class of techniques to identify a particular sample among many similar samples. Biometrics is by far the most popular technology that fingerprints a specific person by using features of a human body. Fingerprinting has many security applications because to identify a unique sample is the foundation of integrity.

A subclass of fingerprinting focuses on mass-produced artificial products. Such a technique has many applications including supply-chain integrity, forensic investigation, and device authentication. So far, researchers have proposed fingerprinting of commodity products based on image processing of target textures: papers by Buchanan et al. \[1\] and Clarkson et al. \[2\] and metallic component such as nuts by Takahashi and Ishiyama \[3\]. Other researchers have studied the technique called RF fingerprinting that fingerprints radio transmitters by observing their radio wave \[4\]. This remote fingerprinting enables a receiver to identify a particular transmitter, and it is useful for thwarting some analogue-domain attacks, e.g. relay attack \[4\].

Light-emitting diode (LED) is a semiconductor device that converts electrical energy to light \[5\]. LED is pervasively used in electronics products for lighting because of its advantages in cost-effectiveness, long lifetime, and low power consumption. Therefore, the fingerprinting of light from LED has many industrial applications. First, we can use the technique for tracing electronics products having LEDs. That is particularly useful for tracing non-intelligent products such as electronic accessories, supplies, and consumables. Secondly, we can use the technique for identifying a transmitter in visible-light communication (VLC) to thwart analogue-domain attacks in VLC in the same way as RF fingerprinting \[6\].

Despite the possibility of large applications, LED fingerprinting is not straight-forward. We cannot use the conventional image-processing approach \[1–3\] because an LED essentially has one pixel only; we should rely on colour for its uniqueness. LED binning, an industrial practice to ensure the colour variation within a set of LEDs, makes the colour-based fingerprinting even more difficult.

In this Letter, we propose the first LED fingerprinting technique. To address the above problem, we use optical spectra of LEDs; the spectra preserve rich information that is degenerated in RGB colour. The recent small and low-cost spectrometers, enabled by microelectromechanical systems (MEMS), make spectral measurement a cost-effective option \[7\].

So far, researchers have proposed fingerprinting uses a coarse-to-fine strategy. In the first step, we distinguish samples by their part numbers. In the second step, we distinguish a particular sample from many samples of the same part number.

### Experiments

**Setup and preprocessing:** Fig. 2 shows the experimental setup. A stabilised power supply drives the LED, and the light from the LED is captured by a spectrometer from 47.5 cm away. The LED holder and the spectrometer are fixed to a base plate for the reproducibility of experiments. A shielding box covers the entire setup during the measurement. The DC power supply drives the target LED sample with the constant current of 20 mA.

**Proposed method:** In this Letter, we consider white LEDs that are commonly used for lighting. Among many ways to realise white light, combining a blue LED and yellow phosphor material is the most common for its cost efficiency \[5\] (see Fig. 1). The phosphor material absorbs blue light from LED and emits yellow light by photoluminescence. Human eyes recognise the mixture of the complementary colours blue and yellow, as (pseudo) white. This type of LED is called phosphor-converted white LED.

The colour of a white LED is susceptible to a slight manufacturing process variation. To tackle the problem, the technique called LED binning comes into play: the colour of an LED is projected to the dimensional vector \(s = (s_0, \ldots, s_{255})\) that represents the spectrum between 340 and 780 nm wavelength at 256 equal steps. The low-cost spectrometer is composed of a grating and a linear image sensor and is available with a few hundred dollars.

**Table 1:** Target LEDs: ten samples from three different products

| Identifier | Manufacturer       | Part number                  | #Samples |
|------------|--------------------|------------------------------|----------|
| \(L_1\)    | Seoul-Semiconductor | LWS14-BULK                  | 10       |
| \(L_2\)    | OptoSupply         | OSWSDK5111A                  | 10       |
| \(L_3\)    | CREE               | C512A-WNN-C20001             | 10       |

As a preprocessing, the total power of measured spectra, which is susceptible to measurement environment, is normalised: the 256-dimensional vector \(s'(0), \ldots, s'(255)\) that represents the normalised spectrum is obtained as

\[
s'(i) = s(i) \left( \sum_{j=0}^{255} s(j) \right)^{-1}. \tag{1}\n\]

**Fig. 1 Structure and spectrum of phosphor-converted white LED**

The proposed fingerprinting uses a coarse-to-fine strategy. In the first step, we distinguish samples by their part numbers. In the second step, we distinguish a particular sample from many samples of the same part number.
Fingerprinting LEDs with different part numbers: As a first step, we distinguish LEDs by a part number. Fig. 3 shows the normalised spectra in (1) from the 30 samples summarised in Table 1. The horizontal and vertical axes are the wavelength and the normalised light intensity, respectively. There are 30 traces, and their colour corresponds to their part number: blue, red, and green traces represent \( L_A \), \( L_B \), and \( L_C \), respectively.

Fig. 3 Normalised spectra of \( L_A \), \( L_B \), and \( L_C \). Ten samples are measured for each part number. The traces are coloured by a part number.

Fig. 3 shows that there is a distinct difference between \( L_A \), \( L_B \), and \( L_C \) in the yellow region (500–600 nm). There is a particularly large difference around 500 nm which is a boundary between the blue and yellow spectra. Therefore, we can distinguish LEDs by a part number by simple thresholding. The difference can be attributed to different semiconductor processes and phosphor materials.

Fingerprinting individual LED samples: As a second step, we distinguish a specific LED sample from others with the same part number. In this particular experiment, we examine \( L_A \). To check the reproducibility of measurements, each sample is measured for ten times.

To emphasise the small difference, we subtract the total mean from each measurement of the ith sample. The further-normalised spectrum \( \tilde{x}_i^j(l) \) of the ith sample for jth measurement is given by

\[
\tilde{x}_i^j(l) = x_i^j(l) - \frac{1}{10 \cdot 10} \sum_{j=1}^{10} \sum_{k=1}^{10} x_i^k(l).
\]

Fig. 4 shows the normalised spectra defined in (2) for 100 traces: 10 measurements of each of the 10 samples. The region higher than 550 nm is omitted because no significant difference is observed. The traces are coloured by samples. The figure shows that each sample makes clusters. These traces suggest that we can distinguish each sample by using an appropriate distinguisher.

Distinguishing samples using machine-learning classifiers: To evaluate the uniqueness of each sample quantitatively, we classify the ten samples in the previous experiment using classification algorithms. For the purpose, the measured data is classified using nine representative supervised-learning algorithms in the \texttt{scikit-learn} machine-learning library.

Table 2 shows the performance figures of the 10-class classifiers. In Table 2, the success rate refers to the one obtained by averaging the success rates of the leave-20%-out cross-validation. LogisticRegression and KneighborsClassifier show the best results with 99 and 98% success rates. The results show that the individual LED samples are distinguishable at a high success rate with an appropriate classifier.

Table 2: Classification of individual samples using supervised learning

| Classifier               | Success rate |
|--------------------------|--------------|
| KneighborsClassifier     | 0.98         |
| Perceptron               | 0.49         |
| LogisticRegression       | 0.99         |
| GaussianNB               | 0.96         |
| DecisionTreeClassifier   | 0.76         |
| RandomForestClassifier   | 0.88         |
| MLPClassifier            | 0.94         |
| SVC                      | 0.22         |
| AdaBoostClassifier       | 0.31         |

Conclusion: We proposed the first fingerprinting technique of white LED using spectral features. The feasibility of the method is verified through concrete experiments. LEDs having different part numbers can be easily distinguished attributed to the difference in LED fabrication processes and phosphor materials. Individual samples of the same part number are still different in the blue region. By using a machine-learning classifier, ten individual samples can be distinguished at the 99% success rate.

This Letter only covers the feasibility study, and there are remaining works before practical application. In particular, we plan to study (i) additional experiments with a larger number of samples and (ii) performance evaluation as a realistic authentication system.

Acknowledgment: This work is supported by JSPS KAKENHI grant number JP18H05289.

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/). Submitted: 6 June 2019 E-first: 11 October 2019 doi: 10.1049/el.2019.1908

One or more of the Figures in this Letter are available in colour online.

A. Toh, L. Yang, K. Sakiyama and T. Sugawara (University of Electro-Communications, Tokyo, Japan)

E-mail: a.toh15@uec.ac.jp

References

1. Buchanan, J.D.R., Cowburn, R., Jausovec, A.V., et al.: ‘Forgery: fingerprinting documents and packaging’, Nature, 2005, 436, (7050), p. 475.
2. Clarkson, W., Weyrich, T., Finkelestein, A., et al.: ‘Fingerprinting blank paper using commodity scanners’. IEEE Symp. on Security and Privacy, Berkeley, CA, USA, May 2009, pp. 301–314
3. Takahashi, T., and Ishiyama, R.: ‘FIBAR: Fingerprint imaging by binary angular reflection for individual identification of metal parts’, 2014 Fifth Int. Conf. on Emerging Security Technologies, Alcala de Henares, Spain, September 2014, pp. 46–51
4. Danev, B.D.: ‘Physical-Layer Identification of Wireless Devices’. PhD thesis, ETH Zurich, 2011
5. Schubert, E.F.: ‘Light-emitting diodes’ (Cambridge University Press, Cambridge, UK, 2006, 2nd edn.)
6. Plank, H., Holweg, G., Steger, C., et al.: ‘Time-of-flight based optical communication for safety-critical applications in autonomous driving’. Computer Safety, Reliability, and Security (SAFECOMP 2016), Trondheim, Norway, September 2016, pp. 183–194
7. Hamanatsu ‘Mini-Spectrometer Micro Series C12666MA Datasheet’, 2019