Medicine tablet authentication using fingerprints of ink-jet printed characters

Ishiyama, Rui; Takahashi, Toru; Makino, Kengo; Kudo, Yuta; Kooper, Martin; Abbink, David

DOI
10.1109/ICIT.2019.8754966

Publication date
2019

Document Version
Accepted author manuscript

Published in
Proceedings - 2019 IEEE International Conference on Industrial Technology (ICIT 2019)

To appear in ***The 20th IEEE International Conference on Industrial Technologies (ICIT2019)***
Feb 13 – 15, 2019, Melbourne, Australia

Medicine Tablet Authentication Using "Fingerprints" of Ink-Jet Printed Characters

Rui Ishiyama
Data Science Research Laboratories
NEC Corporation
Kawasaki, Japan
r-ishiyama@bl.jp.nec.com

Toru Takahashi
Data Science Research Laboratories
NEC Corporation
Kawasaki, Japan
t-takahashi@hg.jp.nec.com

Kengo Makino
Data Science Research Laboratories
NEC Corporation
Kawasaki, Japan
k-makino@mb.jp.nec.com

Yuta Kudo
Data Science Research Laboratories
NEC Corporation
Kawasaki, Japan
y-kudo@bc.jp.nec.com

Martin Kooper
Faculty of 3mE
Delft University of Technology
Delft, Netherlands
m.p.a.kooper@student.tudelft.nl

David Abbink
Cognitive Robotics, Faculty of 3mE
Delft University of Technology
Delft, Netherlands
D.A.Abbink@tudelft.nl

***Abstract*—Counterfeit drugs have been a serious problem causing damage to people's health over the world. Numerous anti-counterfeiting methods based on tagging have been proposed; however, they suffer from three major issues: (1) tagging is applicable only to packages, not tablets directly; (2) end-users, i.e., patients, cannot inspect the tags; (3) tagging incurs extra costs for manufacturers. This paper describes a new method that we propose for authenticating individual medicine tablets as-is by matching images of printed characters. The printed characters on individual tablets of the same medicine seem the same to human eyes, but each is characterized by tiny unique differences. The contributions of this paper are: (a) to reveal the uniqueness of the characters printed by an actual pharmaceutical-use machine and (b) to propose a practical system to identify individual tablets using image matching. Our system is useful for any patients who want to authenticate a medicine tablet at hand: it only requires a picture with a smartphone camera. Our system is also useful for medicine manufacturers, because the database can be constructed using the existing manufacturing process without incurring additional cost. Our image matching algorithm recognizes very detailed features of the images and is accurate and fast even for a large-scale database. In conducted experiments, 1,000 sample tablets were captured using the same optical setup as an actual medicine manufacturing machine. Obtained results showed that 100% accuracy in individual tablet authentication was achieved.**

Keywords—medicine tablet, authentication, identification, fingerprinting, image matching, Fourier-Mellin phase correlation, physically unclonable function, artifact metrics, anti-counterfeit

I. INTRODUCTION

Counterfeit drugs have been serious threats to people all over the world. Medicine counterfeiting is an organized crime that has reached an industrial scale: it involves an estimated 188 billion Euro yearly, constituting the largest segment in fraudulent goods sold worldwide every year [1]. Even in the most secure markets in the world, it is estimated that at least 1 percent of all drugs in circulation are counterfeit [2]. It is even worse in developing regions such as Southeast Asia [3] and Africa: the proportion of counterfeit pharmaceuticals can rise to 70 percent. According to World Health Organization estimates, about 1 million patients die annually from counterfeit medicines and 450,000 preventable malaria deaths each year are caused by counterfeit medicines [2].

The fight against counterfeiting has also become a major issue in many other industries, and numerous technologies have been proposed to distinguish genuine products from counterfeit ones. Overt marking technologies such as holograms on a drug's packaging have been commonly used. However, counterfeiters are becoming increasingly sophisticated and are learning how to overcome them. For example, they are now able to hack holograms applied to the packages and imitate them with a high level of accuracy. Thus, it is hard for ordinary people to distinguish the genuine from the counterfeit.

Recently, individual identification or serialization with track and trace has been employed as an anti-counterfeiting measure. Track and trace of individual medicines will start being enforced in the EU in 2019 and in the US in 2023. Pharmaceutical industries in developed countries are currently working to construct systems using existing serial marking technologies such as barcodes or RFID. However, these conventional identification technologies can only be applied to packages containing medicines. Since such serial marking can be imitated, there remain numerous risks such as imitated serials, re-packaging, and reuse of packages. These risks can be defended against if the track and trace system governs the supply chain perfectly. However, the drug supply chain in developing countries, unlike that in developed countries, is quite complicated and difficult to control. In developing countries, re-packaging or tablet-wise sales are common and thus cannot be covered.

Another anti-counterfeiting measure is to recognize the physically unclonable features of an object itself for authentication, which is also called physically unclonable function (PUF) [4] or artifact-metrics [5]. Methods have been proposed to capture images of microstructures of paper fibers [6][7]. It has also been proposed to manufacture nano-scale artifacts as unclonable features to be authenticated [8].

Microscopic imaging enables fingerprinting industrial parts [9]. A specially designed microscope was developed to authenticate various kinds of luxury goods using a deep learning technique [10]. However, these conventional object "fingerprinting" technologies require special devices for microscopic imaging with a suitable lighting setup. This limits their accessibility for ordinary people, especially in developing countries. Another problem is that these methods require extra costs for manufacturers to construct a genuine object database for authentication.

Consequently, there is still no solution to authenticate medicine tablets that offers both sufficient accessibility for ordinary people and cost-effectiveness for pharmaceutical manufacturers. Such a solution is needed to enable anyone to authenticate tablets at hand, instantly. This means that tablet inspections must be fully automated without requiring any special skills or devices. Recently smartphones with high resolution cameras have rapidly distributed even in developing countries and are thus a good choice as an inspection device. Another important demand is cost-efficiency for pharmaceutical manufacturers. If the authentication system requires much cost to introduce, it is hard to be adopted in practice.

In this paper, we propose a new solution to provide end-to-end authentication using current printed characters on medicine tablets. The proposed system architecture is illustrated in Figure 1. An image database of "fingerprints" of individual tablets is automatically constructed using an existing manufacturing process, i.e., an actual tablet inspection machine. Then, query images are captured using only a smartphone camera and matched with the database images. This architecture offers both cost-effectiveness for pharmaceutical manufacturers and sufficient accessibility for all patients.

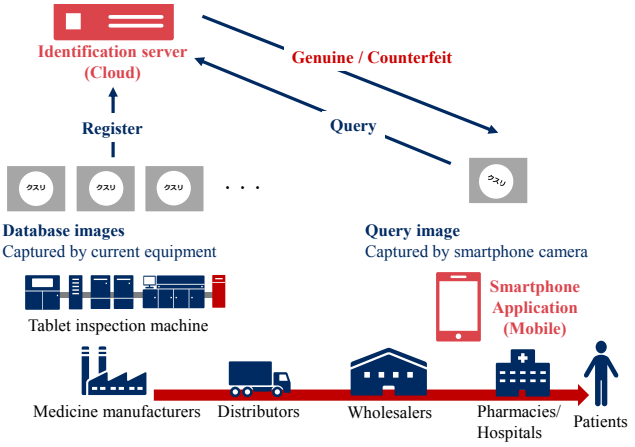

Fig. 1. Architecture of our system for medicine tablet authentication. A database is constructed using an existing tablet inspection machine. Query images are captured using only a smartphone camera. A cloud server stores the database, receives query images and conducts image matching.

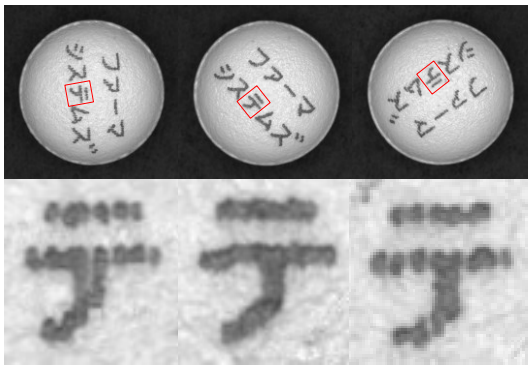

Fig. 2. Tablet images captured by the same optical setup as an actual medicine tablet inspection machine (top row). These images are used for quality inspection at the end of manufacturing. Cropped and magnified local images show the uniqueness of the same characters (bottom row).

II. Proposed Architecture

A. Individual Uniqueness of Printed Characters on Tablets

Recently, ink-jet printers have been adopted by many pharmaceutical manufacturers because they are low-cost and applicable to various kinds of tablets. Printed characters identify the medicine name for preventing misuse by patients.

Figure 2 shows images of printed characters on sample medicine tablets. These images are captured by the "industrial" setup, which is the same as that used by an actual tablet inspection machine. The zoomed images in the bottom row show the individual uniqueness of the same characters. Note that the tablets used in our study are test samples used to testify to the actual medicine manufacturing process. These tablets are made of the same base material and by the same process, but the actual medical components are excluded. Thus the printed name is a dummy one.

Although the printed characters are precisely controlled to make all the individual characters the same for the same medicine, their individual uniqueness can still be seen in the figure. We consider this to be due to micro-scale surface irregularities and small fluctuations in the orientations of tablets being printed, which are apparently uncontrollable and random. In this paper, we propose to use the uniqueness in the printed characters as unclonable features, called "fingerprints", of tablets for individual identification and authentication.

One of this paper's contributions is revealing that these differences are individually unique (never identical among different individual tablets) and distinctive. Thus they are a useful way to achieve highly accurate authentication. Experiments described later show that the uniqueness enables individual tablets to be authenticated with high accuracy, i.e., with equal error rate (EER) less than 10e-6.

It is important to note that these "fingerprints" are generated with zero cost for genuine manufacturers, but that they are very expensive for counterfeiters to imitate. It is almost impossible to imitate these tiny features intentionally; such imitation would at least require a far more costly printing machine than that used in the genuine process. Consequently, this makes counterfeiting unprofitable.

B. *Database Construction Using Existing Manufacturing Process*

Our proposed system is beneficial because it can add a tablet-wise authentication function to existing manufacturing processes without any modification or extra cost for database construction. Ink-jet printing machines are widely used in many existing manufacturers. Visual quality inspections are also widely used for quality assurance. These inspections actually capture the appearance of tablets for inspection with sufficient resolution to ensure that no tablets have any cracks or damage and that the characters to identify the type of medicine are properly printed. In the existing systems, the images are used only for inspection purposes. Our proposed system adopts these images as the database images of the genuine tablets for authentication. Thus, manufacturers do not have to modify their manufacturing process as-is; this makes it quite easy to adopt our proposed system without extra costs.

C. *Cloud-based Authentication by Capturing Query Image Using Smartphone*

Since the previous methods use nano-scale artifacts or microscopic images as "fingerprints", special devices including a microscopic lens and a special lighting setup are necessary to capture query images for authentication. Although several methods provide low-cost devices, their accessibility is still limited for general people. Without a special lens and/or lighting instruments, it is difficult to capture micro-scale surface roughness as "fingerprints" in general environments (see Figure 3). In contrast, our printed character "fingerprints" can be easily captured using only a standard smartphone camera.

Figure 4 shows tablet images captured using only a smartphone camera in various indoor environments, i.e., under ambient light with an only slightly controlled directional light (top row). In comparison to the images captured by the industrial setup (Figure 2), the image quality captured by a smartphone camera is somehow degraded. However, the details of the characters are captured (bottom row). In the experiments described later in Section IV, we will verify that the quality is sufficient for accurate individual identification.

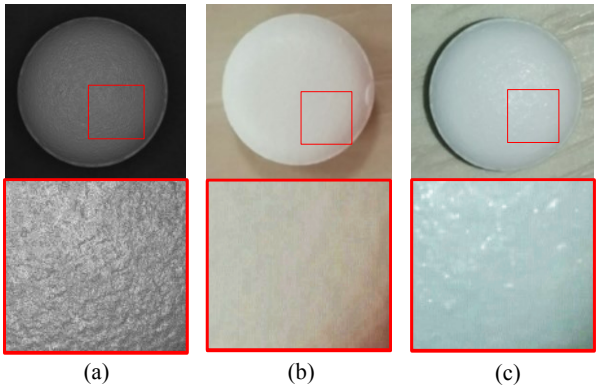

Fig. 3. Images of tablets without printed characters captured using (a) an industrial camera and light setup, (b) only a smartphone camera, (c) a smartphone camera with a flashing built-in LED light (top row). Note that the surface roughness "fingerprints" cannot be captured in images (b) and (c) (bottom row).

Fig. 4. Tablet images captured using only a smartphone camera (top row). Note that small details of the characters can be captured (bottom row).

Fig. 5. Capturing query images using only a smartphone camera. Our simple GUI app helps non-expert users capture query images in an orthogonal view with suitable scaling and centering.

III. Image Matching Method

We assume that the database and query images are captured under rigid transformation including any planar rotation and small amounts of translational and scale changes. The medicine inspection machine has a camera that is fixed orthogonal to the conveyor, and tablets are automatically conveyed so that they are centered in the camera field of view. This is also possible when capturing query images using a smartphone. Users have only to put a tablet on a desk and hold their own smartphone orthogonal to it. A simple GUI app running on the smartphone helps users to center and zoom properly for capturing with easy operation (Figure 5). Most recent smartphones have a camera with high enough resolution to capture the ink-jet printed character "fingerprints."

Consequently, our problem is matching images under any rotation and for any small changes in scale and translation. The algorithm must also be able to extract very small differences as the matching features, and the online matching process has to be completed within a few seconds for a large database of authenticated tablets. The Fourier-Mellin band-limited phase (FMBLP) matching algorithm [11][12][13]

suitably meets these requirements. In the following parts of this section, we will review the algorithm proposed in [13].

A. Geometric Invariant Feature Extraction

First, we convert an input image $f(n_1, n_2)$ into a feature (2D complex array) using Fourier-Mellin Transform (FMT), which gives rotation, scale and translational invariant features. Let $F(k_1, k_2)$ denote the 2D DFT of the input image. FMT is implemented by applying the log-polar transform (LPT) to the amplitude spectrum $|F(k_1, k_2)|$. Our method uses $\log_{10}\{|F(k_1, k_2)| + 1\}$ instead of $|F(k_1, k_2)|$. FMT transforms rotation and scale changes in an image into translational shifts of the resultant image. The feature we obtain by applying LPT to the amplitude spectrum $\log_{10}\{|F(k_1, k_2)| + 1\}$ is denoted by $F_{LP}(k_1, k_2)$; we call it a "Fourier-Mellin transformed (FMT) image."

Next, we apply the 2D DFT to the FMT image $F_{LP}(k_1, k_2)$ and normalize its amplitude spectra as

$$V_f(l_1, l_2) = \frac{\mathcal{F}(F_{LP}(k_1, k_2)}{|\mathcal{F}(F_{LP}(k_1, k_2)|} = e^{j\theta_f(l_1, l_2)}, \quad (1)$$

where $\mathcal{F}(\cdot)$ means 2D DFT operation and $e^{j\theta_f(l_1, l_2)}$ is a phase component of the FMT image $F_{LP}(k_1, k_2)$. We call $V_f(l_1, l_2)$ the Fourier-Mellin Phase (FMP) feature.

Finally, we select only the low frequency bands from the FMP feature $V_f(l_1, l_2)$. Since the high frequency bands in the FMP feature tend to be inaccurate in LPT, we can improve the matching accuracy by this selection. The selected bands of the FMP feature are called the Fourier-Mellin Band Limited Phase (FMBLP) feature.

B. Feature Matching

Our method utilizes DFT-based correlation calculation in order to obtain a matching score; i.e., the correlation value between the query and the database FMBLP features. Let $V_{db}(l_1, l_2)$ denote an FMBLP feature registered on a database and let $V_q(l_1, l_2)$ denote a query FMBLP feature. The cross-power spectrum of these features is described as

$$R(l_1, l_2) = V_{db}(l_1, l_2)\overline{V_q(l_1, l_2)} = e^{j\theta_{db}(l_1, l_2)} e^{-j\theta_q(l_1, l_2)}, \quad (2)$$

where $\overline{V_q(l_1, l_2)}$ means a complex conjugate of the query FMBLP feature $V_q(l_1, l_2)$. The correlation map $r(k_1, k_2)$ between the registered FMBLP feature $V_{db}(l_1, l_2)$ and the query FMBLP feature $V_q(l_1, l_2)$ is given as

$$r(k_1, k_2) = \mathcal{F}^{-1}\{R(l_1, l_2)\} \quad (3)$$

where $\mathcal{F}^{-1}\{\cdot\}$ means 2D IDFT. We employ the peak value of the correlation map $r(k_1, k_2)$ as matching score s between the registered FMBLP feature $V_{db}(l_1, l_2)$ and the query FMBLP feature $V_q(l_1, l_2)$

$$s = max\{r(k_1, k_2)\} \quad (4)$$

Here, we assume that the images (printed characters on tablets) are unique and random for each individual tablet. The shape of correlation map $r(k_1, k_2)$ has a sharp peak like a delta function if the database FMBLP feature $V_{db}(l_1, l_2)$ and the query FMBLP feature $V_q(l_1, l_2)$ are extracted from the same individual tablet. Otherwise, the correlation map $r(k_1, k_2)$ does not have a sharp peak. Therefore, we can identify individual tablets by using the peak value of the correlation map $r(k_1, k_2)$ as a similarity measure.

IV. Experiments

We used 1,000 sample tablets on which the dummy name of the medicine is printed by an actual pharmaceutical-use name printing machine. The sample tablets were of the type actually used for testing actual medicine tablet manufacturing processes. Although they do not contain an actual medical component, their base material, shape and surface condition are exactly the same as those of real medicine tablets. We assume that query and registration images are captured under different orientation, because setting their orientation precisely for capturing is hard for general users who want to authenticate a tablet at hand.

A. Collecting Images Using Industrial Camera and Lighting Setup

We collected database images of 1,000 sample tablets by using the automated scanning system shown in Figure 6. This system is equipped with an industrial-use camera (Omron Sentec Co., Ltd., STC-MBE132U3V), a lens (VS Technology Corporation, VS-TCH05-65CO), a ring LED light (CCS Inc., HPR2-50BL) and a stage driven by stepping motors and a controller (Sigma Koki, Co., Ltd., OSMS33-300 and SHOT-304GS). This camera and light setup simulates the "industrial setup" used in an actual medicine tablet inspection machine. We used this system instead of an actual inspection machine because the latter cannot keep the ground truth of individual IDs for query capturing; it stores the captured tablets randomly into a bucket.

Once we lined up the tablets on the XY moving stage, the stage automatically conveyed each tablet under the camera and automatically captured their "fingerprint" images. First, we placed 7 x 6 = 42 tablets on the stage and captured the images of them (Figure 7). Then we removed the tablets and stored them into a partitioned case while keeping them in the same order. We repeated this process 43 times to capture all 1,000 tablets for the database. Next, we removed the tablets from the partitioned case in the same order, placed them onto the stage, then captured a further 1,000 query images.

This process simulates realistic situations where the orientation of the tablets cannot be set to be the same between the database and query images. Examples of the captured images are shown in Figure 8. Note that 1,000 database images and 1,000 query images were captured in different orientations. Each genuine pair, i.e., a pair of database and

query images of the same individual tablet, had random changes in rotation. The size of the images was 512 x 512 pixels. Actual tablet size was 9.2 mm in diameter, which was 424 pixels in the images.

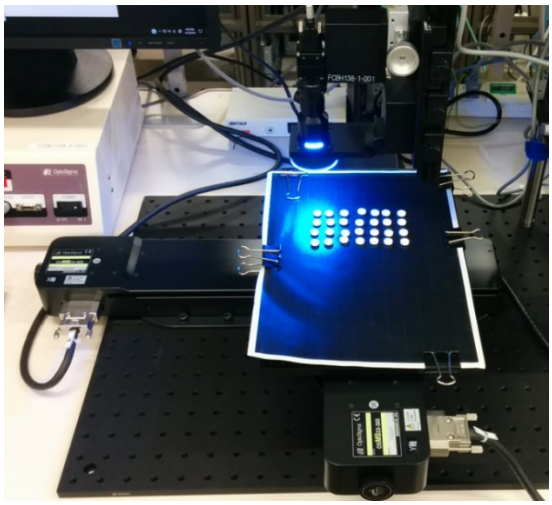

Fig. 6. Capturing system for image collection using a camera and light with the same setup as that used in an actual medicine tablet inspection machine.

Fig. 7. Arrayed tablets. We can keep the ground truth of individual tablet IDs between the first (database) and the second (query) turns of image collection.

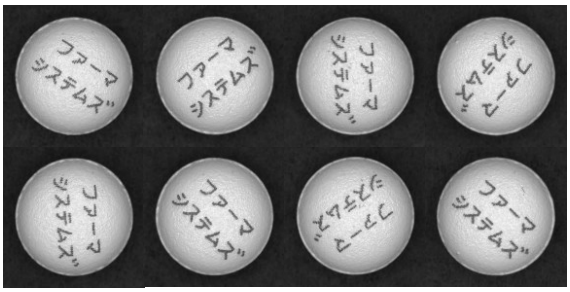

Fig. 8. Examples of query images (top row) and database images (bottom row) captured by the industrial camera and lighting setup. Genuine pair images are shown in the same column.

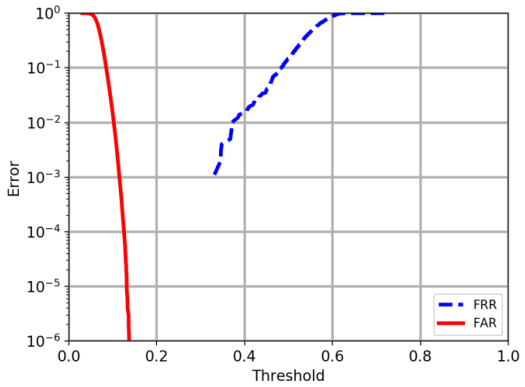

Fig. 9. Cumulative distribution ratio of matching scores of imposter pairs (solid line) and genuine pairs (dotted line). The plots mean respectively false acceptance rate (FAR) and false rejection rate (FRR).

B. Identification Accuracies Using Industrial Setup

We evaluated the uniqueness of the individual printed characters using the image matching algorithm described in Section III. In the algorithm, we selected 200 × 200 phase components around the DC component in the band-limited technique for matching.

In this experiment, one query image of an individual tablet was matched with one database image of the identical tablet and 999 database images of different tablets. Consequently, we matched 1,000 genuine pairs and 999 x 1,000 = 999,000 imposter pairs. Identification accuracy was evaluated by the false acceptance rate (FAR) and false rejection rate (FRR) when a threshold value was applied to the matching score to determine whether or not the query is identical to the matched one in the database.

The experimental results are shown in Figure 9. It shows the cumulative distribution ratio of matching scores of imposter pairs (solid line) and genuine pairs (dotted line). These indicate respectively the false acceptance rate (FAR) and the false rejection rate (FRR), when the threshold value of the x-axis is applied. These results show the wide gap between the FAR and FRR plots, which means that our method succeeded in identifying all 1,000 individual tablets perfectly using a fixed threshold value around 0.2. In addition to achieving perfect identification accuracy, our method running on a desktop computer (CPU: Intel Core i7-4790 3.6 GHz, memory: 32 GB, OS: Windows 7 Professional SP1 64 bit) completed 1-vs-1,000 matching within 976 milliseconds.

C. Identification Accuracies Using Smartphone Camera

In this experiment, we evaluated identification accuracies of the image matching algorithm described in Section III when the query images are captured by a smartphone camera. As shown in Figure 4, the “fingerprints” of the ink-jet printed characters on medicine tablets can be easily captured by a standard smartphone camera. However, the image quality is somehow degraded due to uncontrolled illumination and optical resolution limitations. In this experiment, we randomly sampled 100 tablets and captured images of them using a Google Nexus5 smartphone camera and a simple GUI app (Figure 5). The captured images are shown in the top row of Figure 10. The resolution of the images was 512 x 512 pixels.

Then these query images were matched with the 1,000 database images: 100 genuine pairs and 99 x 1,000 = 99,000 imposter pairs were matched. The database images and the matching algorithm were the same as those for the experiments described in Section IV (B). Identification accuracy was evaluated by the false acceptance rate (FAR) and false rejection rate (FRR).

The experimental results are shown in Figure 11. Although the scores of the genuine pairs became lower than those in Figure 8 due to the lower query image quality, the FAR and FRR plots were still completely separated. This means that our method succeeded in identifying all individual tablets perfectly using a fixed threshold value of 0.149. Since the algorithm was the same, 1-vs-1,000 matching was again completed within 976 milliseconds. These results show that our system works well with the use of a smartphone.

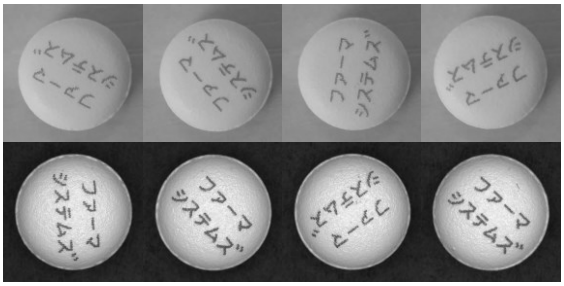

Fig. 10. Query images captured using a smartphone under uncontrolled lighting (top row), and database images captured using an industrial setup (bottom row; same as the bottom row of Figure 8) . Genuine pair images are shown in the same column.

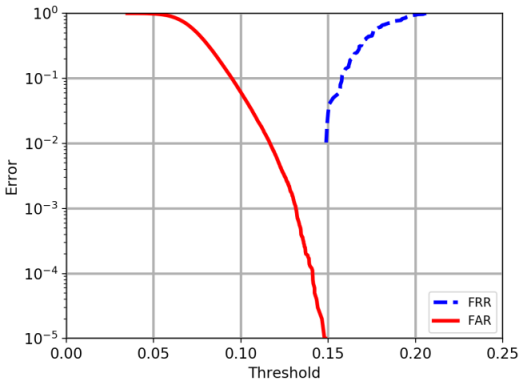

Fig. 11. Sample query images captured using a smartphone camera under uncontrolled lighting conditions (randomly chosen indoor environments).

V. Conclusion

This paper proposed a new system for authenticating medicine tablets as-is by matching "fingerprints" images of ink-jet printed characters. The printed characters on individual tablets of the same medicine seem identical to human eyes, but each has tiny unique differences. These act as "fingerprints" that can be detected by pictures with regular smartphones.

Experiments we conducted showed that the characters printed by an actual pharmaceutical-use machine are so unique that we can identify individual tablets using image matching. It was also shown that the Fourier-Mellin band-limited phase (FMBLP) matching algorithm achieves perfect identification of 1,000 tablets within 976 milliseconds. It was also shown that the "fingerprints" of printed characters can be easily captured using only a smartphone camera and useful for achieving the perfect identification accuracy. Thus our system is useful for any patients who want to authenticate a tablet at hand. Our system is also useful for pharmaceutical manufacturers because the image database can be constructed automatically using the existing manufacturing process without additional cost.

Our future work will be to improve the robustness of authentication accuracy for images captured in uncontrolled environments. This will include optimizing the image matching algorithm to compensate for the differences in image quality between industrial setups and smartphone cameras. It will also include developing a better app to help unskilled users interactively capture good quality images.

References

[1] K. Degardin, Y. Roggo, P. Margot, "Understanding and fighting the medicine counterfeit market," Journal of Pharmaceutical and Biomedical Analysis, vol. 87(18), January 2014, pp. 167–175.

[2] P. Behner, M.L. Hecht, and F. Wahl, "Fighting counterfeit pharmaceuticals: New defenses for an underestimated and growing menace," PWC Report, June 29, 2017.

[3] M. Hussain Khan, J. Okumura, T. Sovannarith, N. Nivanna, H. Nagai, M. Taga, N. Yoshida, M. Akazawa, T. Tanimoto, K. Kimura, "Counterfeit Medicines in Cambodia: Possible Causes," Pharmaceutical Research, 28(3), 484–9, Mar. 2011.

[4] R. Pappu, "Physical One-Way Functions," Science, Vol. 297, 2002.

[5] H. Matsumoto, T. Matsumoto: "Clone Match Rate Evaluation for an Artifact-Metric System," IPSJ Journal, vol. 44, no. 8, pp. 1991-2001, 2003.

[6] J.D.R Buchanan et al., "Forgery: 'fingerprinting' documents and packaging," Nature, vol. 436, no. 7050, 2005.

[7] D. Brzakovic et al, "Authentication of random patterns by finding a match in an image database," Image and Vision Computing, vol. 14, no. 7, pp. 485–499, July 1996.

[8] T. Matsumoto et al., "Nano-artifact metrics based on random collapse of resist," Scientific reports, vol. 4, p. 6142, 2014.

[9] T. Takahashi, R. Ishiyama, "FIBAR: Fingerprint imaging by binary angular reflection for individual identification of metal parts," in Proc. of the 5th Int'l. Conf. on Emerging Security Technologies (EST-2014). Sep. 2014, pp. 46–51.

[10] A. Sharma, V. Srinivasan, V. Kanchan, L. Subramanian, "The Fake vs Real Goods Problem: Microscopy and Machine Learning to the Rescue," Proc. of the 23rd ACM SIGKDD Int'l. Conf. on Knowledge Discovery and Data Mining (KDD '17), pp. 2011–2019, 2017.

[11] Q. Chen, M. Defrise, F. Deconinck, "Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition", IEEE Trans. PAMI, vol. 16, no. 12, pp. 1156–1168, 1994.

[12] K. Ito, T. Aoki, H. Nakajima, K. Kobayashi, T. Higuchi, "A palmprint recognition algorithm using phase-based image matching", Proc. the 2006 IEEE Int. Conf. Image Processing (ICIP), pp. 2669–2672, 2006.

[13] R. Ishiyama, T. Takahashi, K. Makino, Y. Kudo, "Fast image matching based on Fourier-Mellin phase correlation for tag-less identification of mass-produced parts, The 6th IEEE Global Conference on Signal and Information Processing (GlobalSIP), pp. 380–384, 2018