An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code

Yulong Yan, *Graduate Student Member, IEEE*, Zhuo Zou, *Senior Member, IEEE*, Hui Xie, Yu Gao, and Lirong Zheng, *Senior Member, IEEE*

***Abstract*—This article presents an Internet-of-Things (IoT) anti-counterfeiting system that uses visual features combined with the quick response (QR) code. The visual features guarantee the authenticity of a product with the QR code for tracking and tracing. Two visual features, i.e., natural texture features and printed micro features are exploited in the proposed system. The natural texture features use the texture of fiber paper to achieve physical unclonable function (PUF), while the micro features are artificially generated for improved industrial manufacturability and reliability. Features are generated and registered in the production phase when the QR code is printed. In the anti-counterfeiting verification phase, the feature obtained through the feature extraction algorithm is compared with the record to calculate similarity, which indicates the verification result. Such an approach is fully compatible with the QR code-based logistic process without any additional manufacturing cost. A user-friendly application has been developed on a mobile platform that facilitates easy-to-use and affordable devices for verification, such as a mobile phone or a handheld code reader. The experimental results show 99.6% and 99.9% accuracy of anti-counterfeiting verification for texture features and micro features, respectively. The system with corresponding algorithms and software has been demonstrated in real-life products.**

***Index Terms*—Anti-counterfeiting, feature extraction, Internet of Things (IoT), quick response (QR) code, visual feature.**

I. Introduction

COMBATING counterfeiting is a global challenge. The volume of counterfeit products accounts for 3.3% of total world trade, which greatly impedes economic development and endangers society [1]. Fake products are often produced in sweatshops, in violation of child labor laws and fundamental human rights [2]. Counterfeiting of food and medicine leads to more serious issues. Approximately 10% of medicines in low- and middle-income countries are falsified, causing up to 300 000 childhood deaths each year [3]. The amount of single seized fake food reaches 10 000 tonnes and that of fake drinks amounts to one million liters [4]. Therefore, affordable and easily deployable technologies of anti-counterfeiting that are compatible with underlying product tracking and tracing system without additional manufacturing process and cost, are highly desired.

Emerging technologies of the Internet of Things (IoT) have enabled the development of anti-counterfeiting methods that can track and trace products from the source to the end-user, thus controlling fraud throughout the logistic process. Radio frequency identification (RFID) tags [5], [6] are widely considered for tracking and tracing through the product identities (IDs) they provide. However, RFID tags are expensive and require reading devices. Barcode, such as QR code is a pervasive ID carrier, which can be easily read and tracked throughout the supply chain without additional requirements [7], [8]. However, the printable graphical code is proved to be cloneable [9]. Nguyen *et al.* [10] solved this problem by adding a watermark, yet the watermark mode is still crackable. Visual features have powerful anti-counterfeiting effectiveness, which can be divided into natural features and artificial features. Natural texture features are considered to have complete physical unclonable function (PUF). Buchanan *et al.* [11], [12] extracted textures from the surface of this article by laser, of which the high equipment cost is unaffordable. On the other hand, Samsul *et al.* [13], [14] proposed a static laser surface authentication technique which reduces the cost of Buchanan's method, yet the sensitive nature of the procedure renders the method unfeasible to be implemented for general use. Wong and Wu [15] used mobile phone cameras to acquire paper textures. However, the proposed method requires several fixed illumination angles, which is not friendly to unprofessional users. Artificial features created by holograms [16] or ultraviolet ink [17] can be applied for anti-counterfeiting yet will increase the production costs. Pu *et al.* [18] created a novel artificial steganography anti-counterfeiting feature by printing, whose analysis does not take account of anti-copying capability. Inspired by the above works, the introduction of visual features can enhance the security of the QR code.

This article proposes an anti-counterfeiting IoT system that uses visual features combined with QR codes. As shown in Fig. 1(a), the visual features guarantee the authenticity of products, while the QR codes provide the ID for traceability. These features with QR code can be acquired by mobile phone before it is verified and tracked in the cloud. Fig. 1(b) and (c) shows the two adopted anti-counterfeiting visual features: 1) the texture features and 2) the micro features. The texture features require special paper material. They utilize the natural texture

Manuscript received May 13, 2020; revised October 9, 2020; accepted October 20, 2020. Date of publication November 3, 2020; date of current version April 7, 2021. *(Corresponding authors: Zhuo Zou; Lirong Zheng.)*

Yulong Yan, Zhuo Zou, and Lirong Zheng are with the School of Information Science and Technology, Fudan University, Shanghai 200433, China (e-mail: ylyan17@fudan.edu.cn; zhuo@fudan.edu.cn; lrzheng@fudan.edu.cn).

Hui Xie and Yu Gao are with the BOSCH Corporate Research department, Asia-Pacific, Bosch (China) Investment Ltd., Shanghai 200042, China (e-mail: robert.xie@cn.bosch.com; yu.gao2@cn.bosch.com).

Digital Object Identifier 10.1109/JIOT.2020.3035697

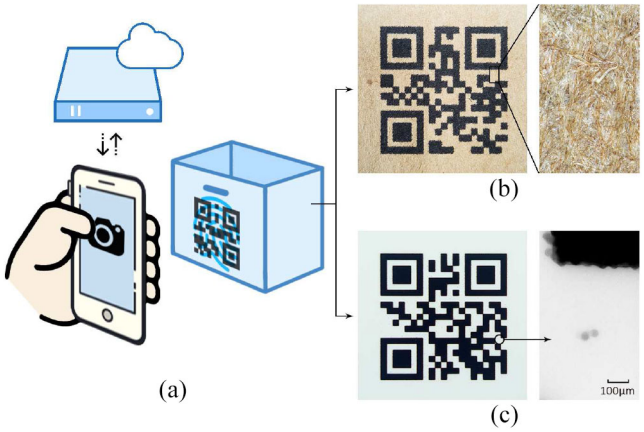


Fig. 1. (a) Illustration diagram of using the anti-counterfeiting system. The verification application acquires visual features with QR code. The cloud server verifies the features and feedbacks the result. (b) Texture features combined with QR code and its microgram. (c) Micro features combined with QR code and its microgram.

of the fiber paper surface to achieve complete PUF. The micro features are generated by printing micron-level ink dots which cannot be perfectly imitated by photocopy machines or scanners. The proposed system is affordable and deployable. The generation process of these features can be adapted to the existing assembly line, without extra cost for manufacturers. The easy-to-use verification application can be deployed on consumer-level end devices like mobile phones or handheld code readers. The verification approach is fully compatible with the logistic process based on QR codes. The system with corresponding algorithms and software has been demonstrated. In the experiment, the verification accuracy of texture features and micro features reached 99.6% and 99.9%, respectively, showing the reliability in anti-counterfeiting.

The remainder of this article is organized as follows. In Section II, the framework of the proposed anti-counterfeiting system and the related algorithms are introduced. Section III describes the image acquisition and assessment on the mobile application. In Sections IV and V, the algorithms for texture features and micro features are detailed, respectively. In Section VI, the performances of the system are evaluated. In Section VII, we summarize this work.

II. System Concept and Related Algorithms

A. System Framework

The system framework, as illustrated in Fig. 2, can be divided into two phases: 1) the visual feature generation and 2) the anti-counterfeiting verification. Visual features combined with the QR code are generated and registered on the assembly line during manufacturing. The verification phase can be carried out throughout the logistic process by a mobile phone or a professional portable device. The features are acquired by the mobile application and compared with the preregistered record in the generation phase.

The anti-counterfeiting based on the natural texture features is depicted in Fig. 2(a). In the feature generation phase, the QR code is printed onto the package or label. The natural texture features of the fiber paper achieve complete PUF. The image is photographed by an industrial camera on the assembly line and registered in the database. The product thus carries such a QR code with security efficacy and will be transported via the supply chain. Anti-counterfeiting verification can be performed in the supply chain timely from the source to the end consumer. During the verification phase, the mobile application can not only acquires the QR code with texture feature, but also assesses the image quality. Only qualified images will be uploaded to the cloud server for further verification. The visual features are compared with the registered record linked to the ID of the QR code. The similarity from the verification algorithm indicates the verification result.

The anti-counterfeiting based on the micro features is shown in Fig. 2(b). During the visual feature generation phase, a set of microdots with high randomness is embedded in the digital printing file. The QR code associated with the artificially added micro features is then printed onto the package or label. Such an approach can eliminate the need for industrial cameras without any additional process or material during manufacturing. Thus, it is cost effective while providing anti-copying capability. Micro features can be selectively encrypted by homomorphic encryption (HE) [19] before being sent to the cloud, further improving the system security without affecting verification.

The most common attacks for QR codes are primarily considered in this work. False attacks refer to printing the same QR codes using the same or similar material, which is considered for the texture feature. Because the texture features are proved to be complete PUF [20], the proposed system can still detect such attacks even if the counterfeiter prints the same QR codes on the fiber papers from the same supplier. The replication attack is considered for micro features. It refers to simply scanning and printing the QR code with micro features, which may deceive the verification.

Fig. 3 illustrates the application and service platform in this work. A mobile application has been developed on Android for the end device as demonstrated in Fig. 3(a), which provides the image acquisition and is detailed in Section III. The role of the application in the system is to guide the user to capture the image, embed algorithms to check image quality, and provide user interaction. The service platform deployed in the cloud includes the database, the algorithm engine for feature extraction and verification, and product tracking and management system for enterprises, as shown in Fig. 3(b).

B. Related Algorithms

Algorithms for the image quality assessment (IQA), feature detection, statistics, and machine learning used in this work, are briefly introduced here.

IQA is used to assess the image quality and remove unqualified images that are affected by light conditions or improper user operations. IQA algorithms consist of blind-IQA and reference-IQA. Specifically, the blind-IQA evaluates an image without involving reference images, while the reference-IQA assesses an image by comparing the image with its reference. Blind/referenceless image spatial quality evaluator

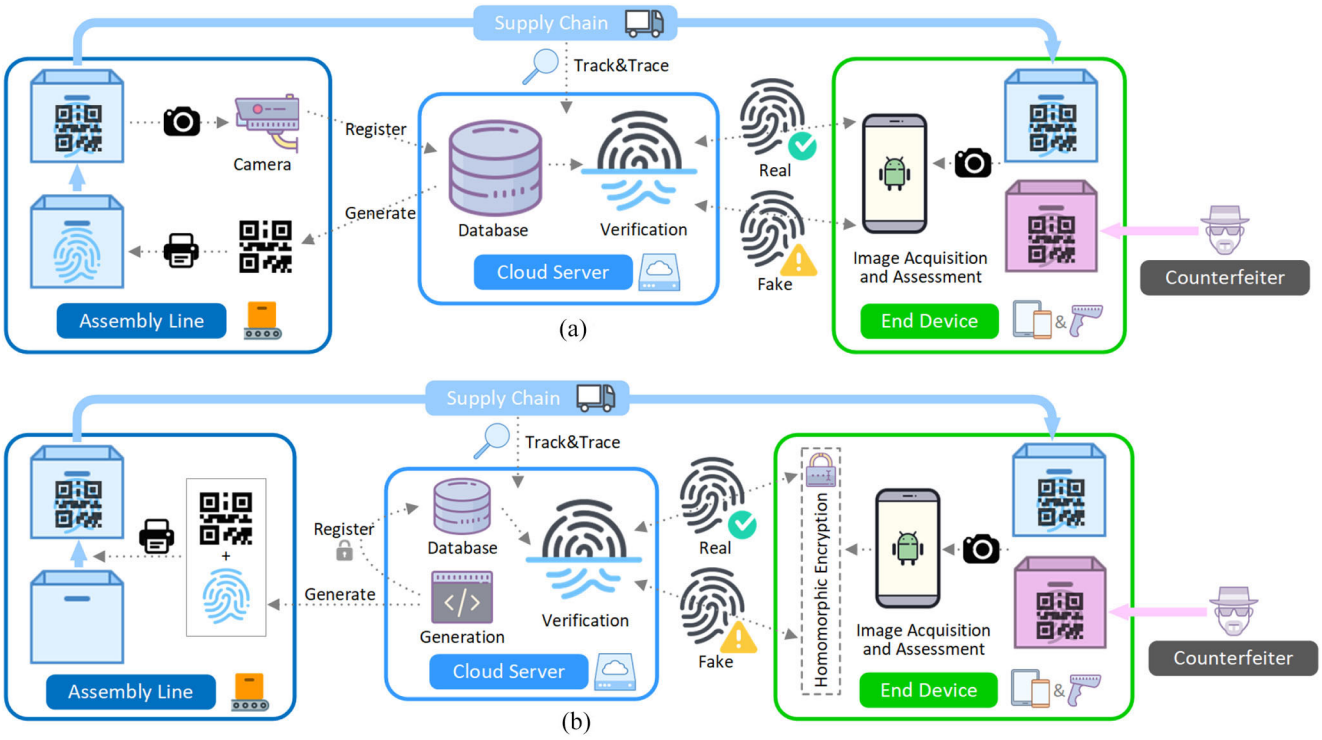


Fig. 2. Proposed anti-counterfeiting system framework of (a) texture feature and (b) micro feature.

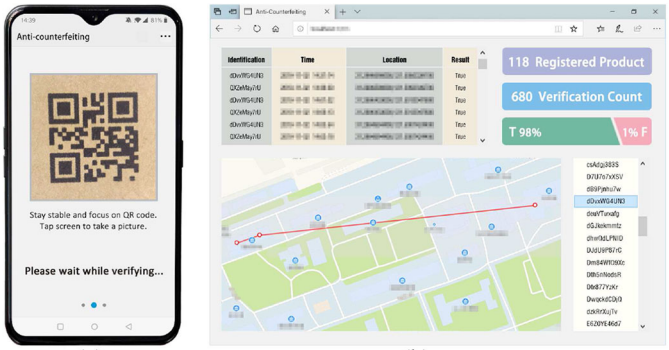


Fig. 3. (a) Mobile application on the end device. (b) Product tracking and management system on the service platform.

(BRISQUE) [21] is a blind-IQA, which predicts IQA score by using a support vector regression model trained on an image database with the corresponding differential mean opinion values. It offers the advantage of the capability to evaluate various types of degradation at the same time, which is similar to the human subjective evaluation of images. Gradient magnitude similarity deviation (GMSD) [22] and structural similarity (SSIM) [23] are both reference-IQA. GMSD calculates the gradient magnitude similarity with the input image and the reference as the assessment result. SSIM measures the similarity between two images from three aspects of brightness, contrast, and structure to obtain the score. Compared to BRISQUE, GMSD and SSIM have lower computational complexity and are more sensitive to structured image degradation.

Feature detection detects and describes the local features in the image. It is employed to extract texture features in this work. Feature detection is generally based on the template or partial differential equation (PDE). Template-based feature detection has advantages in computational efficiency. For instance, features from accelerated segment test (FAST) [24] is based on a circular template containing 16 pixels. Binary robust invariant scalable keypoints (BRISK) [25] applies the corner detector in scale spaces to locate potential interest features. Binary robust independent elementary features (BRIEF) [26] provides a binary feature descriptor without involving the feature detection algorithm. Oriented FAST and rotated BRIEF (ORB) [27] combines the optimization of FAST and the rotated version of BRIEF, which is widely used in real-time feature detection. In contrast to template-based detection, PDE-based detection is better performed in terms of feature robustness. Scale invariant feature transform (SIFT) [28] locates features with the difference of the Gaussian pyramid and the Hessian matrix. Speeded up robust feature (SURF) [29] accelerates this process by approximating the determinant of the Hessian matrix with box filters. However, the Gaussian pyramid does not preserve the natural boundaries of objects, resulting in the loss of feature details. KAZE [30] constructs the scale pyramid by nonlinear local adaptive diffusion filtering to preserve boundaries. Furthermore, accelerated-KAZE (AKAZE) [31] proposes fast explicit diffusion (FED) to accelerate the construction of scale pyramid and modified local difference binary (MLDB) as a selectable descriptor, leading to simplified computational complexity. The computational efficiency and the robustness to texture features are metrics for feature detection, which will be discussed in Section IV-A.

Statistics and machine learning algorithms are also used in the proposed system, mainly in the classification of

TABLE I
EVALUATION OF THE IQA ALGORITHMS

Type	BRISQUE [21]	GMSD [22]	SSIM [23]	Edge Width	Squareness	Size
Qualified	-0.32	0.24	0.94	5.01, 5.37	0.99	1851
Dark	**7.67**	**0.30**	**0.89**	4.76, 5.03	0.98	1909
Blur	**29.29**	0.28	0.95	**10.05, 10.19**	0.99	1938
Skew	**1.50**	0.28	0.94	7.61, 9.16	**0.69**	2217
Small	**34.70**	0.28	0.97	5.80, 6.42	0.99	**1007**

image assessment (Section III), verification of texture features (Section IV), and verification of micro features (Section V). The support vector machines (SVM) [32] is a generalized linear classifier based on supervised learning. In the IQA process, it is used to determine whether the image is qualified to be further verified. Mahalanobis distance [33] is a distance measurement that provides a statistical correction of Euclidean distance. It measures the data similarity in consideration of the scale inconsistency and correlation of the data dimensions. The decision boundary on the Mahalanobis distance is calculated to verify the texture feature, i.e., the texture feature that falls inside the decision boundary is considered true. Otsu [34] is a global optimal threshold based on statistics and is widely used in image binarization. Otsu divides the histogram of the gray image into two categories with the largest between-class variance. It is utilized to extract the micro feature in this work. 2-D Otsu [35] extends the second dimension of the average gray value of the pixel neighborhood on the basis of Otsu in order to achieve a better segmentation effect. K-means [36] is an iterative unsupervised clustering algorithm that clusters data points with shorter distances together. 2-D Otsu and K-means are considered for noise suppression of micro features in the proposed system.

III. IMAGE ACQUISITION AND ASSESSMENT ON MOBILE APPLICATION

In the verification process, the user captures the feature images with the QR codes by the end device, as shown in Fig. 2. The quality of the feature images heavily affects the reliability of the anti-counterfeiting verification. Thus, a mobile application on Android is developed to assist users to capture qualified feature images. Besides, embedded processing for IQA is integrated into the application. It assesses the image quality and removes the unqualified images, thus eliminating the unnecessary transmission to the backend.

A. Mobile Application

The application is deployed on Android for end devices like mobile phones or dedicated portable devices, as shown in Fig. 3(a). The function of the application is to: 1) guide the user to capture the image. The frame finder helps to calibrate the QR code position and prompts a series of photographing guidance, such as focusing and stabilizing; 2) embed IQA algorithms with an SVM classifier to remove unqualified images locally rather than transmitting all photos to the backend; and 3) provide the user interface for verification services, for example, verification results and logs.

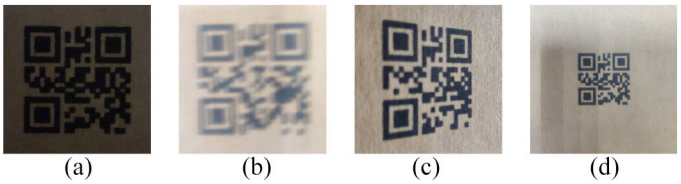


Fig. 4. Types of degraded images due to light conditions and improper user operations.

B. Image Quality Assessment

IQA module is embedded in the Android application for on-device processing. It decreases the verification errors due to image quality degradation and avoids unnecessary communication with the cloud, improving response time and system efficiency. Multiple IQA algorithms comprehensively evaluate image quality, yielding a multidimensional vector as the IQA scores. The SVM classifies the IQA scores into a binary result, i.e., qualified or unqualified. Only qualified images are uploaded to the cloud backend for further verification. Unqualified images are removed, and the application prompts the user to retake the photo.

Degraded images quality caused by light conditions and improper user operations are summarized as the following types. Dark images [Fig. 4(a)] are usually caused by shadow or lack of lighting, while blur images [Fig. 4(b)] are caused by shaking. The tilt of the camera angle and the overlong shooting distance can lead to the case of skew [Fig. 4(c)] and small [Fig. 4(d)], respectively. To evaluate different types of quality degradations, multiple IQA algorithms are exploited in this work, as described in Table I. BRISQUE is similar to human subjective evaluation providing a comprehensive assessment for types of degradation. However, BRISQUE is not a degradation-specific algorithm and is found to be insensitive to degradation types, such as dark and skew. Therefore, computationally lower cost IQA algorithms are adopted as a supplement. GMSD and SSIM assess the structural degradation of pictures in the dark image. Edge Width is the pixel width of the QR code boundary in the x and y directions, reflecting the edge spread caused by blur. Squareness is the area of the QR code divided by the minimal bounding square area, which effectively describes skew images. Size is the average side length of the QR code, indicating small in size.

The IQA scores form a multidimensional vector, and SVM is then used as a binary classifier. Thanks to the IQA, the more reliable feature images lead to a 4.2% improvement in the verification accuracy (the detailed experiments will be presented in Section VI-C). Afterward, the QR code region of the qualified image is cropped and normalized to a square image on end devices to avoid the influence of perspective distortion and size

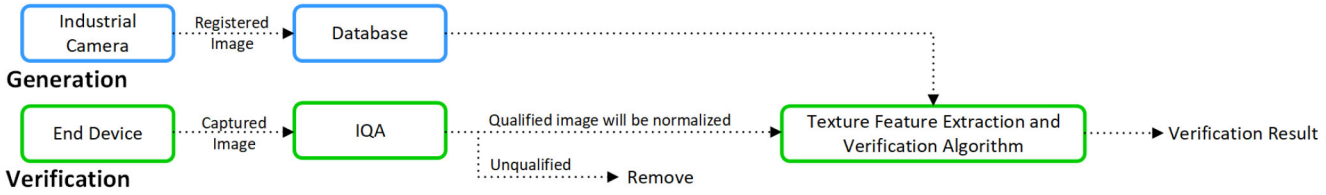


Fig. 5. Method of texture feature extraction and verification. IQA is used to remove the unqualified image. Qualified image is extracted with texture feature and compared with the preregistered image to obtain verification results.

difference. The normalized size of the square image affects texture features extraction and is discussed in Section VI-A.

IV. Texture Feature Algorithm

The random arrangement of pulp fibers inherently forms the texture features during the papermaking process, which is uncontrollable for complete PUF. Thus, the attacker can only use fiber paper from the same supplier to attack. The system is robust to this kind of false attack, showing a high anti-counterfeiting capability.

Fig. 5 shows the proposed method of texture feature extraction and verification. The feature image is acquired by the application on the end device. On-device IQA can eliminate the impact of lighting conditions and improper user operations, ensuring the image quality reliable. The texture feature algorithm uses feature detection and statistical methods to extract and match texture features to output the result of anti-counterfeiting verification.

A. Extraction of the Texture Feature

The texture of the fiber paper surface is a local feature, so feature detection algorithms are used to extract texture features. The feature detection needs to be robust enough to adapt to environmental changes. Meanwhile, it is expected to be computationally economical. Typical algorithms of SIFT, SURF, BRISK, ORB, KAZE, and AKAZE are considered. The repeatability indicates the merits of the detection algorithm, referring to the probability of detecting duplicate features in the same scene. It reflects the robustness of features. The runtime shows the computational burden of the algorithm. Fig. 6 shows that KAZE and AKAZE present the best robustness for texture feature because they use a nonlinear diffusion filter to preserve the boundary of the feature. AKAZE has the fastest speed after ORB, for it uses FED to improve computational efficiency. So, AKAZE is the best feature detection algorithm for the extraction of the texture feature.

B. Verification of the Texture Feature

AKAZE extracts local texture features in the image and expresses them in the form of feature vectors. The vector distance (L2 distance) between two local features indicates their similarity. In Fig. 7(a) and (b), each small circle is an extracted local feature from registered and uploaded images. Feature matching is performed based on the vector distance. The connecting line of the top 50% matches is drawn in Fig. 7(a) and (b). Top 50% is only used for example and not applied in the verification algorithm. The matches in the true texture on

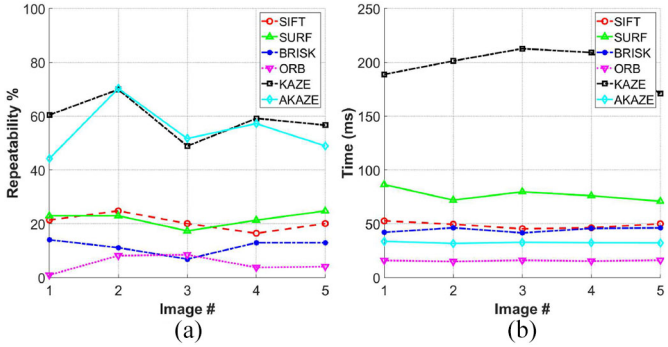


Fig. 6. (a) Repeatability and (b) runtime of different detection algorithms for texture feature.

the upper left are more orderly because the local features correspond to the same positions. The matches in the false texture on the lower left are more chaotic. The histogram of the vector distance makes a better explanation. The vector distance between all matches is counted as a frequency distribution histogram [Fig. 7(c) and (d)]. It can be seen that the first peak of the true texture is closer to 0, which means that the matched local features are pretty similar. The narrower and higher the peak, the more concentrated the similar matches. The first peak of the false texture is far from 0, which means that the matched local features are not similar enough. The peak is wider, indicating a lack of uniformity. The range of the first peak is defined as the index from 0 to the minimum value between the two peak values. The log-normal distribution is used to fit the first peak at the vector distance histogram

$$\mathrm{PDF}(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right) \tag{1}$$

where the variable x represents the vector distance. PDF is the probability distribution function of vector distance subject to parameters μ and σ. The extremum e^{μ} indicates the matching similarity. The logarithmic standard deviation σ indicates the concentration (σ is not the actual standard deviation but its reflection). The expectation $E(X)$ and variance $D(X)$ of the log-normal distribution are related to the estimated parameters μ and σ

$$E(X) = e^{\mu + \frac{\sigma^2}{2}} \tag{2}$$

$$D(X) = \left(e^{\sigma^2} - 1\right) e^{2\mu + \sigma^2}. \tag{3}$$

The exception $E(X)$ and variance $D(X)$ can be estimated on the data X of each set of vector distances to obtain the corresponding estimated values $\hat{E}(X)$ and $\hat{D}(X)$. Therefore, the

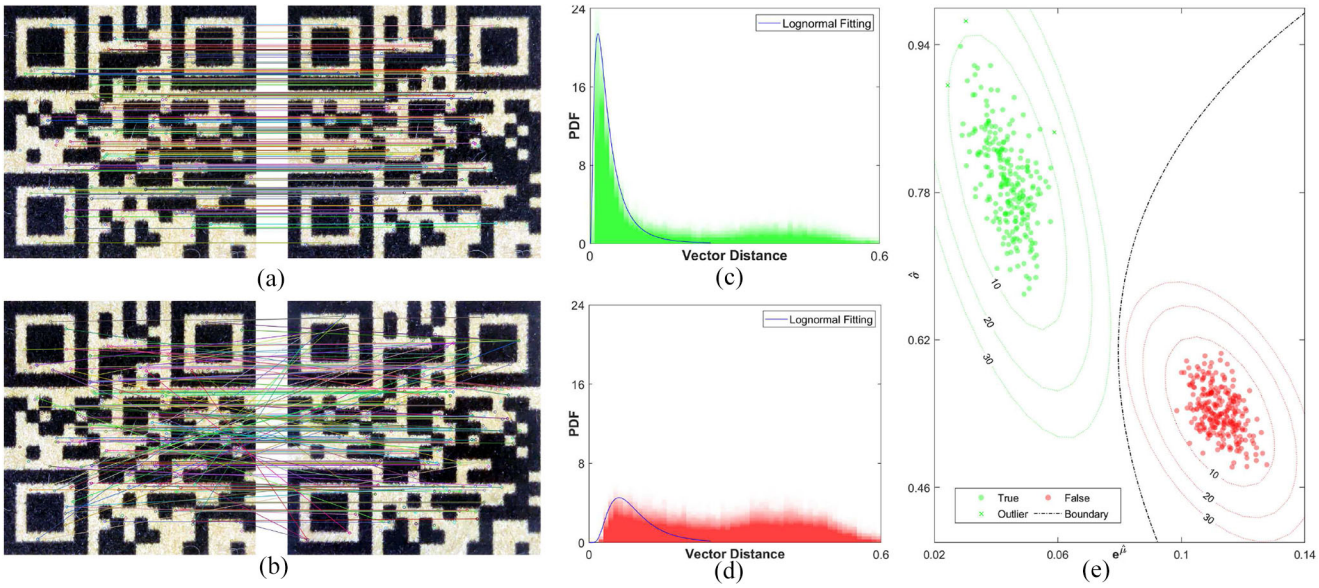


Fig. 7. Result of the top 50% matching in (a) true texture feature and (b) false texture feature. (c) and (d) are corresponding vector distance histograms. (e) Scatter plot of the log-normal parameters, the contour of the Mahalanobis distance, and the decision boundary.

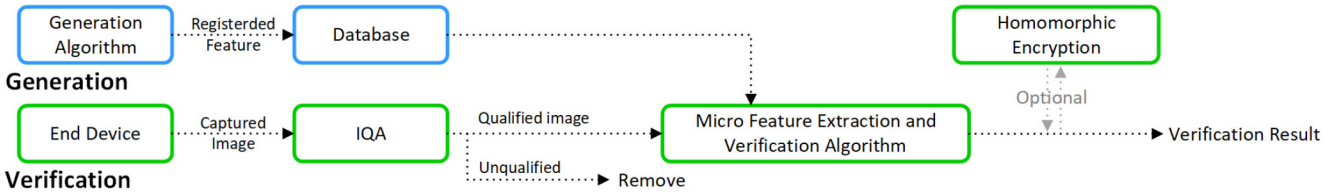


Fig. 8. Method of micro feature extraction and verification. Micro features are extracted and verified on the image that has been removed by IQA. HE is optional in this method and can improve system security.

estimated value $\hat{\sigma}$ and $e^{\hat{\mu}}$ can be calculated as

$$\hat{\sigma} = \sqrt{\ln\left(1 + \hat{D}(X)/\hat{E}^2(X)\right)} \tag{4}$$

$$e^{\hat{\mu}} = \hat{E}(X)/\sqrt{1 + \hat{D}(X)/\hat{E}^2(X)}. \tag{5}$$

The $e^{\hat{\mu}}$ and $\hat{\sigma}$ for 500 true texture images and false texture images are calculated and plotted in Fig. 7(e), which are regarded as two sample sets. The Mahalanobis distance from each point on the plane to the two sets is calculated, which measures the similarity from a point to a sample set. The corresponding contour lines are drawn in Fig. 7(e). The decision boundary is a curve equal to the two samples of the Mahalanobis distance, which is labeled in Fig. 7(e).

In general, for the newly uploaded texture image, texture features are extracted by AKAZE, matched with the registered features. The matched vector distance is fitted with a log-normal distribution to get the indicators $e^{\hat{\mu}}$ and $\hat{\sigma}$. As a result, the authenticity of the product can be determined by observing which side of the decision boundary that the indicator falls into.

V. Micro Feature Algorithm

The printed micro features without the paper material requirements facilitate manufacturability. In this work, the micro features are 100 micron-level ink dots that are randomly printed onto the QR code region. Such tiny ink dots will be massively lost when they are photocopied by copying machines or scanners, which provides micro features with anti-copying capability.

Fig. 8 shows the proposed method of micro feature extraction and verification. In the generation phase, micro features are produced by algorithms and registered directly on the cloud. During the verification phase, IQA is used to ensure the reliability of the micro features. The feature extraction and verification algorithm are executed to obtain the anti-counterfeiting result. Additionally, both registration and verification can be homomorphically encrypted, which is optional and beneficial to improve the security level.

A. Micro feature Generation

The product ID is encoded as a QR code to generate a printing file. 100 microdots are randomly arranged on the white module of the QR code (printing on the black module will affect the reading of QR code) to form micro features. The 2-D coordinate set of 100 microdots are the records of micro features, which are registered on the cloud. The QR code combined with the micro features is printed to the package or label on the assembly line.

B. Extraction and Verification of the Micro features

Microdots as micro features can be extracted by threshold segmentation from grayscale images. The optimal threshold of

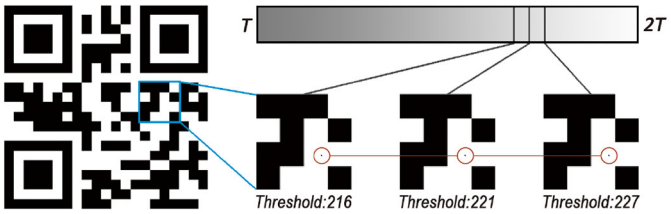


Fig. 9. Thresholding in the micro feature extraction algorithm.

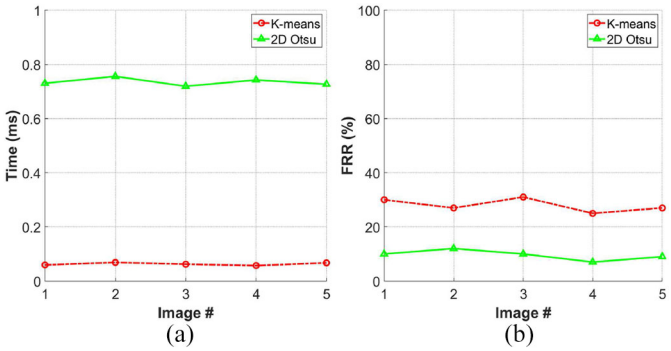


Fig. 10. (a) Time cost and (b) FRR of the pruning algorithm.

microdots is higher than the Otsu threshold T, which separates the black and white modules. Therefore, T and $\min(2T, 255)$ are taken as the start and end of a set of thresholds T_i, taking $0.05T$ as the step length of T_i, to binarize the image in turn (Fig. 9). If an isolated black tiny dot appears stably and continuously in three binary images (as circled in Fig. 9), it is recognized as a microdot. Then its coordinates are recorded for subsequent verification.

When the number of extracted microdots is greater than 100, it means that noisy points are misrecognized and need to be suppressed. K-means and 2-D Otsu are considered. As shown in Fig. 10(a), their time cost is negligible compared to the total running time of several hundred microseconds. The false rejection rate (FRR) is defined as the rate of actual microdots that are erroneously removed, as shown in Fig. 10(b). 2-D Otsu is better in FRR and selected as the noise suppression algorithm.

The previously recorded coordinate set is the evidence used to verify the micro features. Their matching ratio represents the similarity. Euclidean distance between the coordinates of preregistered and extracted microdots is used for one-to-one matching. Then the 3σ rule is adopted to eliminate matches whose distances are too long. The number of matches divided by the number of preregistered microdots is the similarity. Through the experiment to count the similarity of the real products and the fake products, a threshold can be calculated to distinguish them.

C. Verification of the Micro features Based on Homomorphic Encryption

Data security is the primary issue for the enterprise information system. HE is an encryption algorithm that allows mathematical operations on ciphertexts, which can hide data content from the server during verification of features. Therefore, HE is considered in this work, as shown in Fig. 11. As long as the micro features are generated, the coordinates are converted into a binary sequence by the hash algorithm and homomorphically encrypted into a feature ciphertext. On the mobile application, the extracted features are converted into a ciphertext. The cloud server then verifies two feature ciphertexts to obtain the ciphertext result, which is then sent back to the application and decrypted into a plaintext. The server does not know the specific meaning of the data onto the whole process, yet the function of the system can still be realized.

Inspired by perceptual hashing [37] (an algorithm that expresses media as strings to facilitate calculation of similarity), a hash algorithm is proposed to characterize the micro features. The image is divided into $m \times m$ cells, where m is hash resolution. The number of microdots in each cell is represented as an n-bit binary number, where n is called hash precision. As shown in Fig. 12, all cells are presented as a series of binary numbers. In this way, the Hamming distance between binary numbers is the actual difference in the number of microdots.

The binary sequence is homomorphically encrypted as a vector to form the feature ciphertext. The sum of the absolute values of differences between the two cyphertexts is the result ciphertext of the verification. After decryption, the result plaintext is the same as the Hamming distance between the hashed sequences without HE, which can be used to indicate the similarity between two micro features. Therefore, the discrimination threshold can be obtained by counting the Hamming distance of real and fake products.

VI. Experiments and Evaluations

A set of experiments were performed to analyze and optimize the setups and parameters of the proposed system. Their accuracy and efficiency were evaluated. The opensource library of OpenCV 4.1.0. is utilized for computer vision algorithms and the SEAL is used for HE. The QR code reading library is ZBar 0.10. All these programs are running with the Intel Core i7-8750H CPU in the experiments. A OnePlus 7 mobile phone with 48 million pixels camera is used as the end device for deploying the mobile application. In order to facilitate such a system to be compatible with lower end devices for verification, the camera is tuned to be 12 million effective pixels through digital zoom. Fig. 13 illustrates the experimental setup for photographing using a mobile phone and a holder in Sections VI-A and VI-B. The holder is used to control the height and angle to ensure the consistency of the experimental conditions and optimize parameters. The evaluation performed in Section VI-C was on the real-life application on the mobile phone without the holder. The frame finder integrated into the application can guide the user to acquire the QR code.

A. Parameters of the Texture Features

The normalized size mentioned in Section III-B affects the computational burden and performance of texture features. The AKAZE parameters in the texture feature extraction algorithm also need to be selected carefully. The QR codes are normalized to different sizes and various AKAZE parameters are

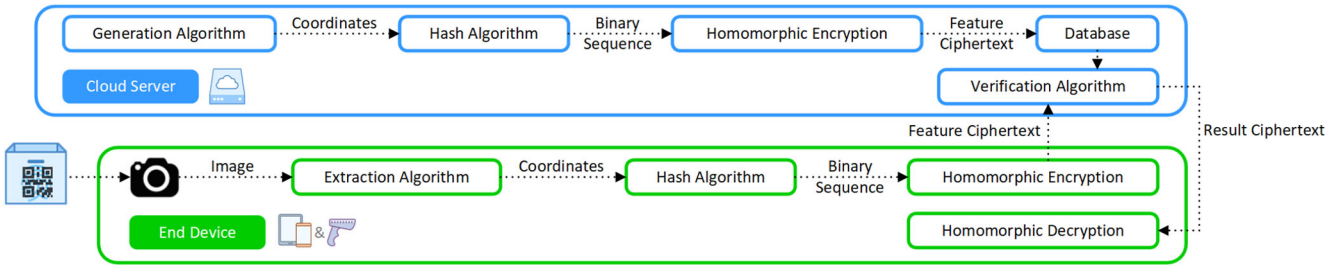


Fig. 11. Framework of micro feature based on HE.

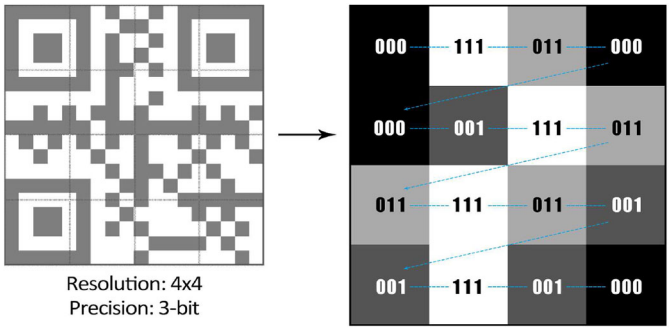


Fig. 12. Micro feature hash algorithm. "000" means no microdot, "011" means two microdots. "111" represents three or more because of the precision limitation. Binary sequence is from left to right and top to bottom.

Fig. 13. Experimental setup for parameter optimization of texture features and micro features in Sections VI-A and VI-B.

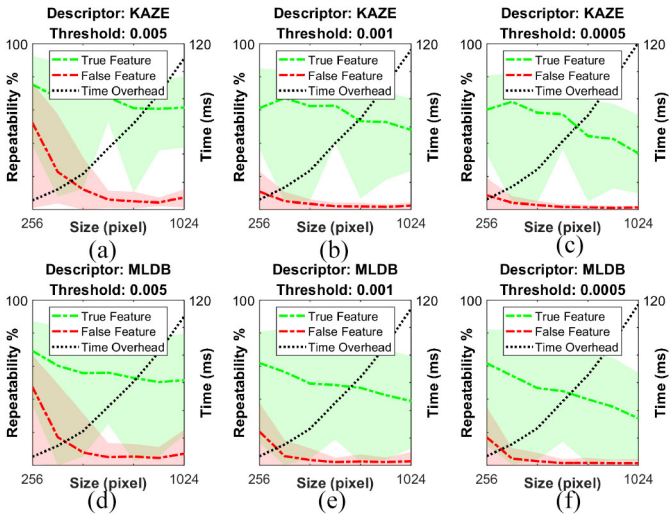


Fig. 14. Algorithm performance under different normalized sizes and AKAZE parameters. KAZE is a float descriptor, and MLDB is a binary descriptor. The threshold accepts keypoints based on the detector response.

used. The impact on the feature repeatability and the runtime are counted on 500 images and shown in Fig. 14. The green and red dash-dot lines are the averages of the repeatability of the true and false features at a specific size. The corresponding light-colored areas indicate their range. The black dotted line is the average of their time overhead.

It is found that the average of repeatability maintains a monotonous trend. However, their range is fluctuating. This is due to improper resizing disturbing the features, resulting in a loss of the true features or misjudgment of the false features. At the smallest possible time cost, a significant margin between the repeatability of the true and false features is expected. And the excessive repeatability of false features means that the algorithm has some instability, which should be prevented. Considering the above principles, the AKAZE parameter in Fig. 14(b) and normalized size 640 × 640 pixels are selected.

B. Parameters of the Micro features

The size of the microdot is crucial to the micro features, as it should not be so large as to be easily counterfeited, or too small to be acquired by the camera. The size can be changed by adjusting the pixel shape in the printing file. The most suitable size can be found through the experiment. The microdots with different pixel shapes are printed out by an EPSON L850 printer at 1440 DPI and measured by a digital microscope. The results are presented in the box-plot of Fig. 15(a), where the corresponding pixel shapes are shown at the bottom. Then micro features are duplicated through the copier to generate replica features. The original features and the replica features are verified with 630 images. Their similarity is shown in Fig. 15(b).

From the experimental results, it can be found that the microdots are greatly lost during copying, hence only a few residues are caught. Moreover, the most significant gap between the original and the replica appears at the pixel shape C. The corresponding size is small and steady (lower size change). Therefore, the pixel shape C is chosen to generate micro features.

The parameters of the hash algorithm affect the accuracy of the micro features under HE. Low resolution leads to position information loss, while high resolution is too sensitive to the microdots on the boundary of the hash cell. The microdots obey uniform distribution, so the precision needs to match the

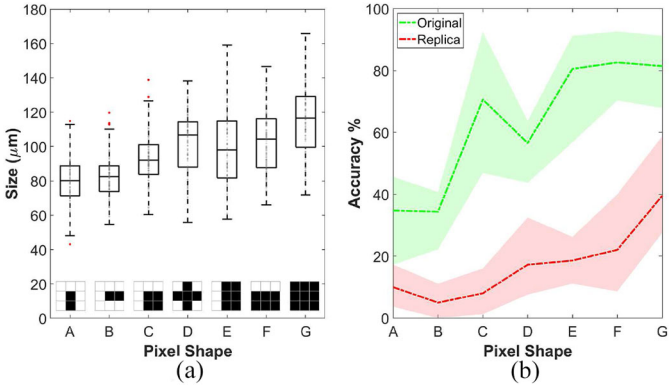


Fig. 15. (a) Microdots size and (b) accuracy for different pixel shapes.

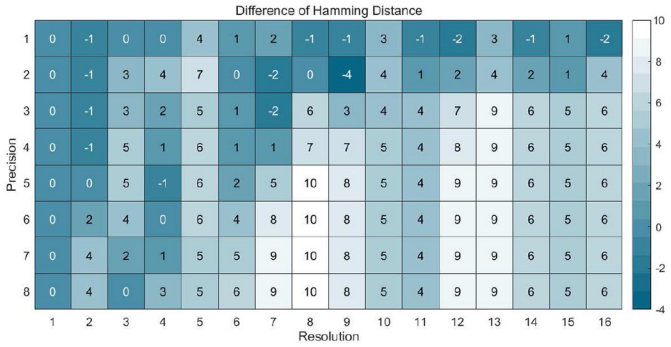


Fig. 16. Hamming distance difference between original and replica in hash parameter space.

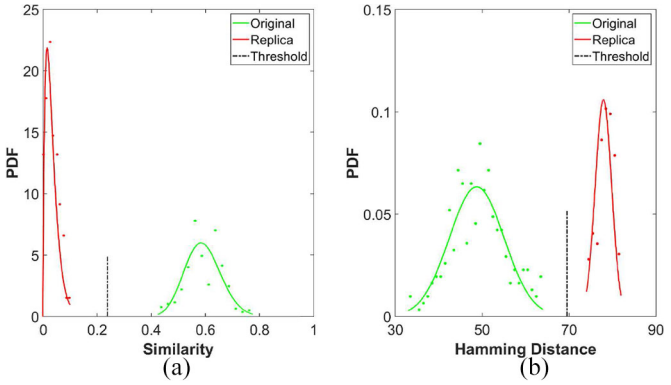


Fig. 17. (a) Similarity of the original and the replica without HE and (b) Hamming distance of the original the replica under HE.

resolution. In addition, properly lowering the precision can improve the robustness to noise and misrecognition.

In the parameter space composed of hash resolution and precision, the Hamming distance interval between the original and the replica is calculated (Fig. 16). The larger the interval, the more reliable and stable the verification. The resolution of 8×8 and the accuracy of 5 bits are proved to be the optimal parameters, bringing the best separation of the original and the replica.

The similarity of the original micro features and the replica micro features without encryption are plotted in Fig. 17(a). The Hamming distances of the original and replica under encryption are plotted in Fig. 17(b). Small Hamming distance means high similarity. In both cases, micro features can be identified by a threshold. Note that after HE, there is still a discernible difference between the original and replica, yet the interval is indeed reduced. This phenomenon shows that HE improves security at the cost of stability.

C. System Evaluation

To evaluate and analyze the performance of the system, the average algorithm runtime, and the accuracy of verification are tested comprehensively and reported in Table II. For feature generation, the size of the QR code is 2 cm $\times$ 2 cm, and the resolution of the printing file is 1440 DPI. All images for verification were captured through the mobile application in the real-life environment. 60% of the images were captured indoors and the rest were captured under daylight at different times of the day.

A total of 680 texture feature images were captured by the mobile application for experiments, 340 among which are false attacks. 571 out of 680 images passed the IQA and were further verified by the system. The testing results demonstrate an accuracy of 99.6% under such attacks. Only 1 out of the 571 images was mistakenly verified from the false attack to the true one, and 1 true image was verified to be false. It is found that the 2 errors were mainly caused by the degradation of image quality.

A total of 737 micro feature images were tested. 370 of them were replication attacks by an ESPON L850 printer at 1200 scan DPI. 706 out of 737 images passed the IQA and were verified. The system verification accuracy under the replication attack reaches 99.9%. Only 1 out of 706 images was mistakenly verified from true to false. It is also found that the cause of this error is the degradation of image quality.

As reported in Table II, the accuracy of verification with IQA on different features is improved by 4.2%, at expenses of approximately 70 ms of time cost to the entire system. It indicates that the system has the ability to eliminate the adverse effects of light conditions and improper user operations.

The runtime of the generation algorithm affects the manufacturing speed. The texture features come from this article material. Their generation time is the encoding time of the product ID. The micro features are produced by algorithms with computational overhead, whose generation time is larger than texture features. The homomorphic encrypted micro features need to be encrypted before feature registration, resulting in an additional time cost of 4.4 ms.

HE improves the system's security when micro feature is used. It only brings a slight time cost with little sacrifice of accuracy. The micro features under encryption still meet the available standards. However, whether to use the encryption step still requires careful consideration in different application scenarios.

The texture feature utilizing the natural texture provides complete PUF. It is computationally intensive for feature extraction (longer runtime) and sensitive to the light and image quality. The micro feature does not achieve complete PUF but enhances industrial manufacturability. Based on the different characteristics of two anti-counterfeiting features, they

TABLE II
EVALUATION OF THE SYSTEM

Type	Generation Time	Verification Time	Verification Accuracy
Texture feature	11.45 ms	318.73 ms	95.4%
Texture feature + IQA		**392.79 ms**	**99.6%**
Micro feature	118.45 ms	149.36 ms	95.7%
Micro feature + IQA		**222.77 ms**	**99.9%**
Homomorphic micro feature	122.83 ms	159.61 ms	95.0%
Homomorphic micro feature + IQA		**234.32 ms**	**99.2%**

TABLE III
SUMMARY OF DIFFERENT ANTI-COUNTERFEITING FEATURES

Type	Advantage	Disadvantage	Application scenarios
Texture feature	Complete PUF	Material requirement Complex computation	Luxury products, e.g. jewelry, red wine and electronics.
Micro feature	Cost effective Short runtime	Not complete PUF	Retail products, e.g. food, beverages and daily necessities.

are designed for different application scenarios, as shown in Table III. The texture feature is proved to be complete PUF, which has the highest anti-counterfeiting effect. It can provide high security for luxury products. The micro feature does not achieve complete PUF. Replication attacks using precise instruments may cause verification errors. Therefore, micro features are suitable for retail products. High attack cost and low profit are the sources of the anti-counterfeiting effectiveness of micro feature.

VII. CONCLUSION

This article presents an IoT anti-counterfeiting system using visual features with QR codes. The visual features guarantee the authenticity of the product with the QR code for tracking and tracing. Two adopted visual features are natural texture features from the texture of the fiber paper and the printed micro features produced by printing micron level ink dots. The texture features provide absolute PUF, while the micro features facilitate industrial manufacturability and reliability. In the generation phase, the visual features combined with the QR code are registered on the cloud service. In the verification phase, the application deployed on the end device acquires the visual feature and uploads it to the cloud. IQA is applied to remove the unqualified image and feature extraction and comparison are performed to obtain the anti-counterfeiting result. The proposed system is fully compatible with QR code-based supply chain without any additional manufacturing cost. A software application has been developed on a mobile platform that facilitates easy-to-use and affordable devices for verification, such as a mobile phone or a portable device. The two visual features have reached 99.6% and 99.9% accuracy, respectively. At the same time, the micro features can be homomorphically encrypted, improving the security of the system and maintaining the accuracy of 99.2%.

REFERENCES

[1] *Trends in Trade in Counterfeit and Pirated Goods*, OECD Publ., Paris, France, 2019.

[2] D. Thomas, *Deluxe: How Luxury Lost its Luster*. New York, NY, USA: Penguin, 2007.

[3] G. M. Nayyar *et al.*, "Falsified and substandard drugs: Stopping the pandemic," *Amer. J. Trop. Med. Hyg.*, vol. 100, no. 5, pp. 1058–1065, 2019.

[4] *Largest-Ever Seizures of Fake Food and Drink in INTERPOL-EUROPOL Operation*, Europol, Hague, The Netherlands, 2016.

[5] Q. Lin, L. Yang, and Y. Guo, "Proactive batch authentication: Fishing counterfeit RFID tags in muddy waters," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 568–579, Feb. 2019.

[6] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1634–1646, Oct. 2017.

[7] Z. Li, G. Liu, L. Liu, X. Lai, and G. Xu, "IoT-based tracking and tracing platform for prepackaged food supply chain," *Ind. Manag. Data Syst.*, vol. 117, no. 9, pp. 1906–1916, 2017.

[8] Y. Peng, L. Zhang, Z. Song, J. Yan, X. Li, and Z. Li, "A QR code based tracing method for fresh pork quality in cold chain," *J. Food Process Eng.*, vol. 41, no. 4, 2018, Art. no. e12685.

[9] O. Taran, S. Bonev, and S. Voloshynovskiy, "Clonability of anti-counterfeiting printable graphical codes: A machine learning approach," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brighton, U.K., 2019, pp. 2482–2486.

[10] H. P. Nguyen, A. Delahaies, F. Retraint, D. H. Nguyen, M. Pic, and F. Morain-Nicolier, "A watermarking technique to secure printed QR codes using a statistical test," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Montreal, QC, Canada, 2017, pp. 288–292.

[11] J. D. Buchanan *et al.*, "'Fingerprinting' documents and packaging," *Nature*, vol. 436, no. 7050, p. 475, 2005.

[12] R. Cowburn, "Laser surface authentication–reading Nature's own security code," *Contemp. Phys.*, vol. 49, no. 5, pp. 331–342, 2008.

[13] W. Samsul, H. P. Uranus, and M. Birowosuto, "Recognizing document's originality by laser surface authentication," in *Proc. 2nd Int. Conf. Adv. Comput. Control Telecommun. Technol.*, Jakarta, Indonesia, 2010, pp. 37–40.

[14] W. Samsul, H. Uranus, and M. Birowosuto, "Static laser surface authentication with low-cost microscope: Tolerances on spatial and angular disturbance," *J. Opt.*, vol. 44, no. 3, pp. 225–232, 2015.

[15] C.-W. Wong and M. Wu, "Counterfeit detection based on unclonable feature of paper using mobile camera," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1885–1899, 2017.

[16] Y. Blau, O. Bar-On, O. Kotlicki, Y. Hanein, A. Boag, and J. Scheuer, "Novel optical materials and applications," in *Proc. Adv. Photon.*, Zurich, Switzerland, Jul. 2018. [Online]. Available: https://www.osapublishing.org/conference.cfm?meetingid=166&yr=2018#NoW1D

[17] L. Cozzella, C. Simonetti, and G. S. Spagnolo, "Drug packaging security by means of white-light speckle," *Opt. Laser Eng.*, vol. 50, no. 10, pp. 1359–1371, 2012.

[18] Y.-F. Pu, N. Zhang, and H. Wang, "Fractional-order spatial steganography and blind steganalysis for printed matter: Anti-counterfeiting for product external packing in Internet-of-Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6368–6383, Aug. 2019.

[19] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," IACR Cryptol. ePrint Archive, Lyon, France, Rep. 2012/144, 2012.

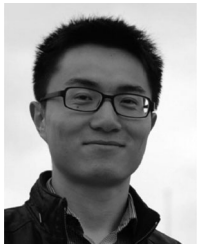
[20] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, "Fingerprinting blank paper using commodity scanners," in *Proc. 30th IEEE Symp. Security Privacy*, Berkeley, CA, USA, 2009, pp. 301–314.
[21] A. Mittal, A. K. Moorthy, and A. C. Bovik, "No-reference image quality assessment in the spatial domain," *IEEE Trans. Image Process.*, vol. 21, no. 12, pp. 4695–4708, Dec. 2012.
[22] W. Xue, L. Zhang, X. Mou, and A. C. Bovik, "Gradient magnitude similarity deviation: A highly efficient perceptual image quality index," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 684–695, Feb. 2014.
[23] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[24] E. Rosten and T. Drummond, "Machine learning for high-speed corner detection," in *Proc. Eur. Conf. Comput. Vis.*, 2006, pp. 430–443.
[25] S. Leutenegger, M. Chli, and R. Y. Siegwart, "BRISK: Binary robust invariant scalable keypoints," in *Proc. Int. Conf. Comput. Vis.*, Barcelona, Spain, 2011, pp. 2548–2555.
[26] M. Calonder, V. Lepetit, C. Strecha, and P. Fua, "BRIEF: Binary robust independent elementary features," in *Proc. Eur. Conf. Comput. Vis.*, 2010, pp. 778–792.
[27] E. Rublee, V. Rabaud, K. Konolige, and G. Bradski, "ORB: An efficient alternative to SIFT or SURF," in *Proc. Int. Conf. Comput. Vis.*, Barcelona, Spain, 2011, pp. 2564–2571.
[28] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, 2004.
[29] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Proc. Eur. Conf. Comput. Vis.*, 2006, pp. 404–417.
[30] P. F. Alcantarilla, A. Bartoli, and A. J. Davison, "KAZE features," in *Proc. Eur. Conf. Comput. Vis.*, 2012, pp. 214–227.
[31] P. F. Alcantarilla, J. Nuevo, and A. Bartoli, "Fast explicit diffusion for accelerated features in nonlinear scale spaces," in *Proc. Brit. Mach. Vis. Conf.*, 2013, pp. 1–11.
[32] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.
[33] P. C. Mahalanobis, *On The Generalized Distance in Statistics*, Nat. Inst. Sci. India, Delhi, India, 1936.
[34] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Trans. Syst., Man, Cybern.*, vol. 9, no. 1, pp. 62–66, Jan. 1979.
[35] J. Zhang and J. Hu, "Image segmentation based on 2D Otsu method with histogram analysis," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 6. Hubei, China, 2008, pp. 105–108.
[36] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. 5th Berkeley Symp. Math. Stat. Probab.*, vol. 1. Oakland, CA, USA, 1967, pp. 281–297.
[37] P. Cano, E. Batle, T. Kalker, and J. Haitsma, "A review of algorithms for audio fingerprinting," in *Proc. IEEE Workshop Multimedia Signal Process.*, St.Thomas, VI, USA, 2002, pp. 169–173.

Yulong Yan (Graduate Student Member, IEEE) received the B.E. degree in communication engineering from Shandong University, Jinan, China, in 2017. He is currently pursuing the Ph.D. degree with the School of Information Science and Technology, Fudan University, Shanghai, China.

He has been working in the field of intelligent electronics and systems since 2016, especially in computer vision, pattern recognition, and machine learning algorithms for anti-counterfeiting and traceability of the IoT systems.

Zhuo Zou (Senior Member, IEEE) received the Ph.D. degree in electronic and computer systems from KTH Royal Institute of Technology (KTH), Stockholm, Sweden, in 2012.

He was the Assistant Director and a Project Leader with VINN iPack Excellence Center, KTH, where he coordinated the research project on ultralow-power embedded electronics for wireless sensing. He is currently with Fudan University, Shanghai, China, as a Professor, where he is conducting research on integrated circuits and systems for IoT and ubiquitous intelligence. He is also an Adjunct Professor and Docent with the University of Turku, Turku, Finland.



Hui Xie received the B.E. degree in automatic control from Northwestern Polytechnical University, Xi'an, China, in 2010, and the Ph.D. degree in robotics from King's College London, London, U.K., in 2014.

He is currently the Head of the IoT@Life Program and Group Leader for IoT & I4.0 with the Bosch Research and Technology Center in China.

Yu Gao received the B.E. degree in telecommunication engineering from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2009, and the M.S. degree in electrical engineering from the University of Queensland, Brisbane, QLD, Australia, in 2012.

He joined RTC5-AP in Bosch Research as a Research Scientist of Computer Vision and Machine Vision topics in Shanghai, in 2018. His research interests are image and video processing, computer vision, machine vision, and deep learning.

Lirong Zheng (Senior Member, IEEE) received the Ph.D. degree in electronic system design from the KTH Royal Institute of Technology (KTH), Stockholm, Sweden, in 2001.

He was with KTH as a Research Fellow, an Associate Professor, and a Full Professor. He is the Founding Director of the iPack VINN Excellence Center of Sweden and has been the Chair Professor of Media Electronics with KTH since 2006. He has been also a Guest Professor since 2008, and a Distinguished Professor since 2010, with Fudan University, Shanghai, China, where he currently holds the Directorship of the Shanghai Institute of Intelligent Electronics and Systems. He has authored more than 500 publications. His current research interests include electronic circuits, wireless sensors and systems for ambient intelligence, and the Internet of Things.