Banknote identification through unique fluorescent properties

Banknote identification through unique fluorescent properties

Renato Ferrero, *Senior Member, IEEE,* Bartolomeo Montrucchio, *Senior Member, IEEE*

Abstract—The use of printed banknotes is widespread despite cashless payment methods: for example, more than 27 billion euro banknotes are currently in circulation, and this amount is constantly increasing. Unfortunately, many false banknotes are in circulation, too. Central banks worlwide are continuously striving to reduce the counterfeiting. To fight against the criminal practice, a range of security features are added to banknotes, such as watermarks, micro-printing, holograms, and embossed characters. Beside these well-known characteristics, the colored fibers inside every banknote have strong potential as a security feature, but have so far been poorly exploited. The mere presence of colored fibers does not guarantee the banknote genuineness, as they can be drawn or printed by counterfeiters. However, their random position can be exploited to uniquely identify the banknote. This paper presents a technique for automatically recognizing fibers and efficiently storing their positions, considering realistic application scenarios. The classification accuracy and fault tolerance of the proposed method are theoretically demonstrated, thus showing its applicability regardless of banknote wear or any implementation issue. This is a major advantage with respect to state-of-the-art anti-counterfeit approaches. The proposed security method is strictly topical, as the European Central Bank plans to redesign euro banknotes by 2024.

Index Terms—ultraviolet light, security features, banknote counterfeiting.

1 Introduction

Currency counterfeiting, i.e. the production of money without the authorization of a national government, is as old a practice as the coining of money [1]. In the 7th century BC, the ancient Greeks were the first people that coined money to pay for goods or services instead of bartering [2]. Solon, an Athenian statesman, drafted the Solonian constitution in the early 6th century BC: among the laws that regulated public and private life, harsh punishments were imposed on coin counterfeiters. Initially, currency included only coins with different nominal values, represented with different weights and materials (such as gold, silver and electrum). Counterfeit coins used to have base metals in their core, and they were covered in a gold or silver coating in order to resemble authentic coins. From the 9th century AD in China, and the 14th century AD in Europe, banknotes were introduced alongside coins. Counterfeiting banknotes quickly became more profitable than counterfeiting coins, due to their higher nominal value and their lower intrinsic value (since paper is used instead of metal).

Traditionally, banknotes were counterfeited by professionals and governments, for example as part of organized crime or for destabilizing foreign economies during wars. However, with the advent of electronic devices such as digital presses and scanners, this illegal activity has also become accessible to non-professional and casual counterfeiters [3]. As a consequence, the central banks have to continuously add or vary security features when printing money. The best-known security features are watermarks, holograms, security threads, and iridescent stripes [4], but there are many more, such as color shifting ink, fine line printing patterns, micro printing, unique serial numbers, etc. While the average customer only checks for the few security features visible to the naked eye, retailers usually exploit authentication devices as they manage large amount of banknotes every day. Authentication devices can be classified into two categories: the first group (which includes ultraviolet lamps, infrared viewers, and magnifiers) supports the user in determining the authenticity of the banknote, whereas the second group automatically signals the genuineness of the banknote with a particular output (red/green light, sound, text, etc.) [3]. Automatic devices are commonly preferred with respect to devices which are human assisted.

Ultraviolet light can reveal some characteristics of the banknote that do not appear in visible light: ultraviolet dull paper, colored fibers (red, blue, green) and some patterns (like the map of Europe lighting up yellowish on the back of euro banknotes). For example, these features are visible in Fig 1, which is the real-size picture of a €50 banknote illuminated with ultraviolet light. Unfortunately, the presence of ultraviolet properties is often considered sufficient for establishing the authenticity of a banknote when manually inspecting it with ultraviolet light, but basic imitations of ultraviolet characteristics can be easily obtained by counterfeiters thanks to wide availability of ultraviolet inks for ink jet printers [5]. As a consequence, the use of ultraviolet light is becoming discouraged among retailers. This is not related to the strength of ultraviolet characteristics, but it depends on improper checking and misjudging. In order to solve this issue, an approach for automatizing the authentication of banknotes according to their ultraviolet properties is described here. By implementing the proposed technique in an auto detection device, every banknote can be unequivocally identified, and human errors would be eliminated.

The basic idea of the proposed approach is to exploit the fibers inside the banknotes, which are visible only with exposition to ultraviolet light. The fibers are small

Authors are with the Dipartimento di Automatica e Informatica, Politecnico di Torino, Italy. E-mail: renato.ferrero@polito.it, bartolomeo.montrucchio@polito.it

Manuscript received Month Day, Year; revised Month Day, Year.

Fig. 1. The ultraviolet image of a €50 banknote.

components randomly disposed inside the paper during its fabrication. This means that every banknote has a different fiber placement. In this way fibers can be mapped uniquely to banknotes as fingerprints with people [6]. The proposed anti-counterfeit approach is strictly topical, as the European Central Bank plans to review the design of euro banknotes by 2024, based on recommendations of European citizens collected and filtered by advisory groups from each European countries [7].

The main contributions of this paper are: the description of four application scenarios that exploit fibers' recognition in order to verify the authenticity of banknotes, a robust image processing algorithm for recognizing fibers in the ultraviolet image of the note, and an efficient encoding technique for storing the main information related to the position of fibers. The remainder of the paper is organized as follows. Related work is reviewed in Section 2. Section 3 discusses the applicability of the proposed anti-counterfeiting method. The implementation details for the authentication and unique identification of banknotes based on the fibers' position are presented in Section 4. The information encoding is described in Section 5 and the classification accuracy is theoretically computed in Section 6. Results are provided in Section 7. Finally, some conclusions are drawn in Section 8.

2 Related work

The most common approaches for recognizing and authenticating banknotes evaluate features appearing in visible light, i.e., with wavelength in the range of $400 - 700$ nm [8], [9], [10]. Image analysis with different wavelengths usually provides complementary information. In particular, this section reviews state-of-the-art solutions for banknote analysis that exploit ultraviolet imaging. Three main approaches can be identified, as shown in Fig. 2.

The first methodology consists in illuminating the banknote with an ultraviolet light source and then measuring the amount of light emitted by the banknote. The emission

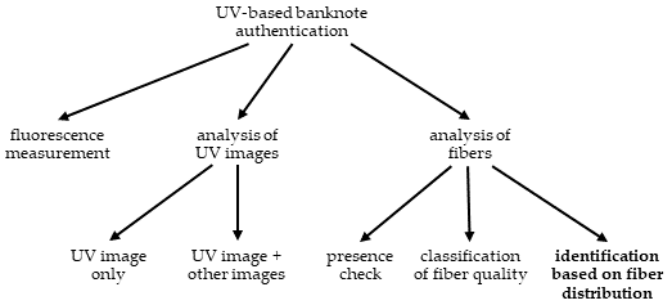


Fig. 2. Taxonomy of approaches for banknote recognition and authentication based on ultraviolet image analysis.

of light by a substance after absorbing a higher energy level of light is called *fluorescence*. Fluorescence measurement is commonly exploited in patents of fake note detector machines [11], [12], [13]: usually, the emitted light is measured in the visible spectrum [11], [12], but the light in the ultraviolet spectrum can be evaluated as well [13]. The level of fluorescent light is compared with predefined thresholds in order to check the authenticity of the banknote.

The basic steps of the second technique are illuminating the banknote with an ultraviolet light source, taking a picture of it, and then analyzing the ultraviolet image as a whole, without discriminating among inner details. This procedure is commonly adopted for automatically recognizing the nationality and denomination of banknotes, but it is usually supported with other discriminating features for better accuracy. For example, ultraviolet images are analyzed together with visible and infrared images [14], or with some physical properties, such as size and color [15]. In the former example, all images are managed as 2D arrays and a Fast Fourier transform is applied. The spectrum obtained with the discrete Fourier transform is the input of a nearest neighbor algorithm for the banknote classification. In the latter example, the similarity between the ultraviolet image

and a reference one is computed by comparing the sum of values in corresponding groups of pixels. The mean value of brightness and the size of RGB images of banknotes are the other two inputs of the classification algorithm.

Ultraviolet images can be analyzed also for assessing the authenticity of banknotes. For example, pattern and background in the ultraviolet image can be distinguished by means of a Gaussian mixture model [16]. In this way, tests for counterfeit currency can be implemented more easily on the ultraviolet pattern. Similarly, a feature vector can be obtained by filtering the ultraviolet images of Indonesian rupiah notes with Gabor wavelets of different scales and orientations [17]. A neural network classifies genuine and fake banknotes according to a cosine-based distance measure applied to the feature vector.

In order to certify a banknote, ultraviolet images can be flanked by other kinds of images. For example, pictures of Ethiopian banknotes are taken under ultraviolet and visible light [18]. Both kinds of images are compared with benchmarks. This approach does not consider any specific features in visible or ultraviolet light, but it just computes a similarity score by means of the Cauchy-Schwarz inequality theorem. If the similarity measures is higher than a threshold, then the banknote is recognized as authentic. Another approach evaluates both ultraviolet and latent images (where invisible patterns are revealed by means of proper processing techniques, i.e., convolution and filtration) [19]. In particular, features regarding ink properties and the security thread are extracted from the ultraviolet images. Then, banknotes are classified by a neural network and a support vector machine.

The third kind of analysis is based on the detection of fibers visible at ultraviolet light. This approach is discussed in details because it is the one followed in the current paper. Three strategies can be recognized in scientific literature for determining the authenticity of a banknote based on the detection of its fibers.

The first strategy regards the simple check of the presence of fluorescent fibers, because it assumes that counterfeiters are not able to reproduce ultraviolet fibers. This hypothesis is weak, therefore the detection of fibers is often accompanied by other checks. For example, a tool for authenticating Bangladeshi banknotes looks for the presence of fibers, as well as other five features: micro-printing, watermark, optically variable ink, iridescent ink, and security thread [20]. The banknote is recognized as genuine if at least four features are detected. An analogous approach detects fake Bangladeshi banknote by analyzing fibers, micro-printing and the face of the first President of Bangladesh reproduced on the note [21]. The Hough transformation algorithm is exploited to recognize the presence of fibers. Similarly, the presence of fluorescent fibers is one of the criteria, alongside with watermark and color-changing ink, for verifying the currency of Taiwan [22]. Genuine banknotes are classified according to a support vector machine.

The second strategy acknowledges that fibers can be present in fake banknotes, but they appear significantly different from fibers in genuine banknotes due to the low quality of the counterfeiting process. For example, a neural network classifies fibers in Indian rupees according to their illumination and shapes [23]. Fibers in a rupee are evaluated independently from each other. Since some fibers can be misclassified, a banknote is considered original if the majority of fibers is classified as genuine; vice versa a larger amount of fake fibers indicates a counterfeit banknote.

The third strategy is more robust because it recognizes that fibers can be counterfeited with the same quality of genuine ones. It is the strategy followed in this paper and it has been seldom considered in literature. Only a couple of works process the random distribution of the fibers visible at ultraviolet light in order to uniquely identify euro banknotes [24], [25]. Despite the similarity of the basic idea, the implementation differs from the one detailed in this paper. Firstly, the positions of the fibers are saved in a matrix. Every cell of the matrix is mapped to a group of pixels of the image. The cell is marked with 1 if it contains the whole fiber or a significant portion of it, 0 otherwise. This solution is penalizing in terms of memory space, because the matrix is sparse and useless data (cells without fibers) are stored. Secondly, the similarity between the reference image and the benchmark is evaluated by applying the exclusive OR operator: all pixels of the two images (including the ones without fibers) are processed. Thirdly, the empiric threshold (set to 99%) for evaluating the similarity does not handle properly the variability of the whole process (due to implementation details, light conditions, worn-out banknotes, etc.), as demonstrated in Section 6. Finally, only two application scenarios are considered: the connection with a central database of a verification authority [24] and the printing of new encoded information on the banknote in order to intrinsically identify it [25].

3 Application scenarios

The main goal of the proposed anti-counterfeiting method is to produce a digital signature of every euro banknote with an encoding scheme able to distinguish all circulating euro banknotes, which are several billions. The digital signature is based on the presence of fibers in the banknote. Although this basic idea has already been investigated in scientific literature, existing methods [24], [25] have some limitations. For example, printing the digital signature on the banknote itself [25] could be sufficient only if it were not possible to forge a complete banknote, introducing perfect copies of a single true banknote. A simpler encoding [24] would require a strong investment from the European Central Bank and a permanent Internet connection.

The proposed algorithm is tailored on retailers, as they are the usual target of counterfeiters. Other possible stakeholders are local banks and public citizens, but their demand for an anti-counterfeiting method is lower. In fact, local banks usually do not check the correctness of a single banknote. Commonly, bank clerks leaf through several banknotes by hand in fast succession, in order to find unusual kinds of paper; only when they find a suspicious note, they check fine details of it. But generally speaking, local banks do not check the banknote originality: this task is demanded to the Central Bank. On the contrary, a public person receives few banknotes per day, maybe no more than one or two. He/she has poor qualitative knowledge of the security features [26], [27], but the time that he/she can spend for verification is relative high, e.g., 5 seconds [3].

Retailers stand in the middle: they often manage banknotes during the day, as bank clerks do, but their competence in discriminating true banknotes is poor, comparable to the one of ordinary people. Furthermore, they must evaluate notes quickly, in order to reduce the waiting time of customers. The following desiderata have been identified for an anti-counterfeiting method tailored for retailers [3]:

- the verification time should be lower than 2 seconds;
- the retailer should not rely on a human operational check under an ultraviolet lamp: in the proposed approach, the test is machine based;
- the output of the detector implementing the proposed approach is binary (yes/no);
- the banknote can be inserted in the detector on any side, because it is trans-illuminated;
- the proposed algorithm can be easily adapted using a smartphone, with a custom-made add-on for the ultraviolet translucent lamp.

Smartphone based applications for detecting counterfeit banknotes are already partially available [28], in which the characteristic line-patterns in banknotes are used to verify the authenticity of the banknote.

Different application scenarios for a fibers-based anti-counterfeiting method are proposed, in increasing order of implementation effort:

1) fibers' positions are freely available on the web site of the Central Bank for each banknote. Moreover a program (e.g., an App for smartphones) is available for performing the check, given the image of the banknote. A cryptographic hash function, such as SHA256, is used to provide a digital signature of the correctness of data.
2) fibers are encoded by means of a public/private key system, in particular with the private key of the Central Bank and the public key of the specific reader. Pieces of information corresponding to the different fibers may be differently ordered from reader to reader. In this way, the private key of the Central Bank is not weakened by encoding the same data with many public keys from different readers.
3) fibers' information is encoded by means of the public key of the central bank and private key of the reader. Encoded data are sent via Internet to the Central Bank, which can confirm authenticity or not. A good computational power is required for the reader and a connection with the Central Bank must be always available.
4) no data about the fiber encoding are publicly available, but only SHA256 personalized for every device (or set of devices). A reader computes by itself its own version of SHA256 and compares it with the one from the Central Bank (connection required) or from a local hard disk. Forgery is very difficult.

The first approach is the simplest one and can be applied in different ways, as it requires either an Internet connection or a local hard disk with data for all banknotes. Retailers can use a device for checking banknotes in every moment, because the Internet connection is not mandatory and a fast checking time (lower than 2 s) is guaranteed. The main problem is the possibility of forgery with perfect copies of the original banknote. Traceability of the banknotes is possible only if an Internet connection is available; anyway it is still difficult because the connection is not certified. The security level of the first approach is the lowest one: it corresponds to the minimum requirements that are always met in the other approaches, regardless of any problem may occur. For example, any other scenario where the information of banknotes are stolen downgrades to the first scenario, where the fibers' positions are publicly available.

In the second approach, information about fibers' position is not public. Data can be put in a local hard disk in encoded form, so forgery becomes more difficult (but still possible). In particular if a little known (to the Central Bank) jitter is given to the parameters of the banknotes for each reader, it could be possible, in case of forgery, to understand which reader was used to recover fibers' positions; in fact it is possible to guarantee a good traceability of readers.

The third approach requires the Internet connection. The main advantage is that fibers' positions are never available, with the exception of a little number of banknotes. The channel must be safe in order to avoid attacks like man in the middle. During usage a little database of fibers can be built. Moreover, banknote recognition can be enforced by changing the coding order in each set of readers (e.g., readers from a local bank) and/or by using a single SHA256 digital signature for each banknote (for each reader).

The fourth approach can work both with a local hard disk or with an Internet connection. If an Internet connection is available, with this approach it is possible:

- to verify if a banknote is in two different places at the same time;
- to understand if a banknote in a set is used independently from the others in the same set;
- to track banknotes among persons, e.g., verifying banknotes transits in ATMs.

It should be noted that if a counterfeiter printed an exact copy of a banknote, including all fibers' positions, the system would not be able to distinguish it from the genuine one. However, the difficulty in reproducing all details makes the forgery complex and expensive, so it would be cost-effective only if a large number of copies were printed. When verifying the false notes, the system would detect many times the same banknote in different places, so it may signal the suspicious case. In this way, without accepting the banknote, it is possible to hinder the diffusion of the copies.

In order to recognize and prevent data alteration, both in public server and local hard disk, a checksum (with different techniques, e.g., the methods used for open source programs, like Linux kernel) can be used. Also a blockchain could be used for the purpose.

In the described application scenarios, a permanent Internet connection enables a real-time traceability of the banknotes, but this is not a requirement for the authentication of banknotes. If the connection is occasional, the banknote originality can be checked by exploiting the local database. Then, when an Internet connection is available, the application communicates at the Central Bank the list of banknotes previously tested. At the same time, it can

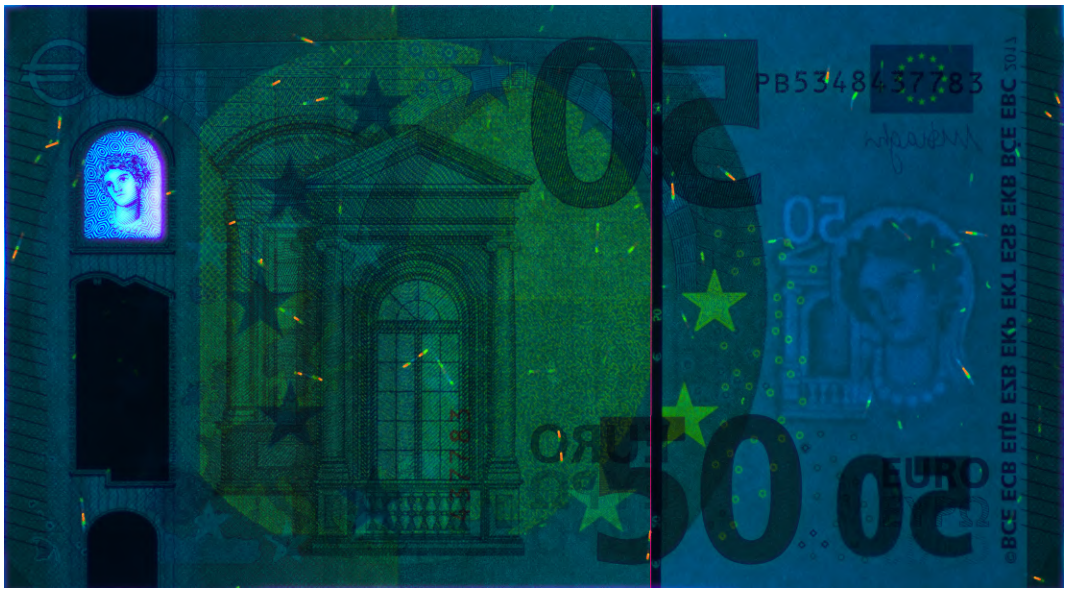


Fig. 3. Highlight of fibers and security thread in the ultraviolet image of a €50 banknote.

download information about any new banknotes printed by the Central Bank, in order to update the local database. More in general, the different approaches are designed in order to offer a graceful degradation of the services. If all resources are available, including a permanent Internet connection and a secure communication channel, the best services are offered, such as real-time traceability and the most effective practices to make forgery extremely difficult. As resources becomes limited, it is still possible to verify the banknotes, but with relaxed constraints on traceability and anti-counterfeiting mechanisms.

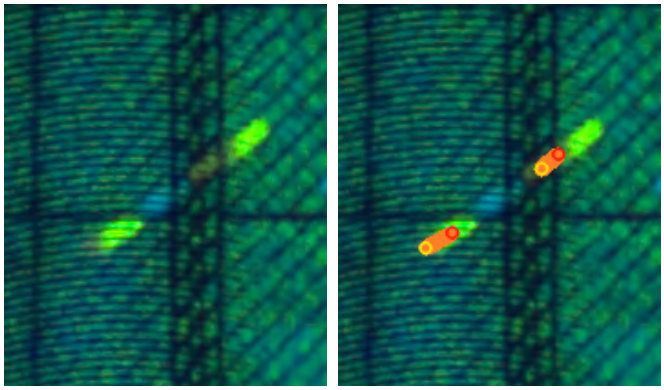
4 Implementation

In the proposed approach, the banknote is illuminated with ultraviolet light and a picture is taken, such as in Fig 1. A computer vision algorithm has been developed to analyze three features appearing in the ultraviolet image: position of the centroids of the fibers, slope of the fibers, and position of the security thread. The algorithm, which is implemented in C++ and exploits some functions provided by OpenCV (Open Source Computer Vision Library) [29], is straightforward: this confirms the ease of implementation and the robustness of the proposed approach. A new image is generated in output, where the three features are highlighted, as shown in Fig. 3. Other elements appearing in the ultraviolet images, such as the fluorescent female portrait or ultraviolet ink marks, are not annotated in the output image: in fact, they do not share the fibers' characteristics which are considered by the algorithm, as detailed in the following.

This paper focuses on the second series of euro notes, called the Europa series due to the presence of a portrait of Europa as security feature. Nevertheless, the approach is valid for a wide range of banknotes all over the world.

4.1 Fiber's centroid search

The first step in the detection of the fiber's centroids is the conversion of the ultraviolet image in the HSV (Hue Saturation Brightness) color space. In fact, some small portions of the banknote have brightness and color similar to the fibers when illuminated by ultraviolet light. For example, the stars in the European union flag in Fig. 1 can be misinterpreted. Therefore, to better distinguish the features in the image, computer vision operations are performed in the HSV color space, instead of using the RGB color space.



(a) Original image (b) Processed image, with fiber highlighted

Fig. 4. Zoomed images of the €50 banknote, before and after the fibers' search.

The image converted in HSV format is then filtered, obtaining a mask with only the desired features. Subsequently, a dilation technique is applied and then a blob detection method is exploited in order to detect the fiber centroids. In computer vision, blob detection methods aim at detecting regions in a digital image that differ in notable properties, such as brightness or color, compared to surrounding regions. Informally, a blob is a region of an image where some properties are (approximately) constant; all points in a blob can be considered similar to each other. In details, in the implementation of the proposed algorithm, the various blobs are located by means of the OpenCV function *SimpleBlobDetector*.

A fiber is composed of some pieces with different colors. We call *subfiber* a part of the fiber with the same color. For example, Fig. 4a and Fig. 4b present a zoom of a fiber (the one inside the doorway) shown in Fig. 1 and Fig. 3, respectively. Red and yellow dots represent the centroids of the two subfibers, giving also the direction. Hue is used to find a direction of the fiber (due to the changing color), whereas saturation (correlated to the color spectrum) is used to help in the recognition. The orange line that connects the centroids is added after the fiber's slope search, as described in Section 4.2. In the proposed approach, the fiber recognition is enhanced using longer fibers composed by two subfibers or more. The subfibers are firstly located and then linked two at a time, saving the distance between them.

4.2 Fiber's slope search

Every fiber is not only characterized by its position, but also by its orientation and slope. Thus, additional information is carried by the angle between the fiber and the horizontal axis. Thanks to the HSV color space, subfibers of different colors are extracted from the fibers. These subfibers, being far enough, permit to calculate the angle α of the fiber, according to the following formula:

$$\alpha = \arctan\left(\frac{y_1 - y_2}{x_1 - x_2}\right) \tag{1}$$

where (x_1, y_1) and (x_2, y_2) are the coordinates of the two subfibers. The angles are then taken within [0,360] degrees.

Fig. 4b shows the centroids of two subfibers and the orange line that connects them.

4.3 Security thread search

The security thread is a black vertical line appearing in the ultraviolet image: in Fig. 1 it can be noted across the two biggest 50 numbers. The position of this line can vary within a range of some millimeters. Therefore, it has been added among the discriminating characteristics of euro banknotes.

With respect to the fiber's centroids, the security thread is easier to find for several reasons. First, it has larger dimensions, as it extends across the whole height of the banknote and is about 5 times wider than a fiber. Secondly, its orientation is fixed: it is vertically aligned, without any slope. Thirdly, it is sensibly darker than the surrounding pixels, so it can not be confused with the background. The search algorithm of the security thread exploits these characteristics. The starting points have abscissa equal to half the length of the banknote and variable ordinate. For each point, the algorithm moves to the right, increasing the abscissa, but keeping the same ordinate. The first point significantly darker than the previous ones is considered the beginning of the security thread. The search is repeated with different ordinate values: as the security thread is vertically aligned, the abscissa of the first dark point slightly varies. Then, the detected dark points are connected with a read line in order to clearly identify the security thread, as shown in Fig. 3. In fact, the search algorithm is so robust that it is repeated only twice: the first time with an ordinate close to the top border of the banknote, and the other time with an ordinate close to the bottom border. Repeating the search more times would increase the fault tolerance of the algorithm, for example in presence of noise, as values of abscissa not coherent with the others can be discarded. However, this would increase the execution time and, above all, false detection of the security threads never occurred during the tests. For the same reason, other checks, such as a minimum amount of consecutive dark points detected, are possible to increase the robustness of the algorithm, but there were no practical needs to implement them. Detailed images of the security thread found in the banknote depicted in Fig. 1 and in two other banknotes are shown in Fig. 9.

5 Proposed encoding

The information regarding the fibers in the banknotes has to be stored in a local or remote database, as detailed in Section 3. A good trade-off between precision of the data and memory occupation is required: although the fibers in a banknote is few (in the order of tens), the number of existing banknotes is huge. A possible encoding of information is presented and then the size of the database is estimated.

First, a unique identifier has to be saved for each banknote, in order to provide a primary key in the database. The natural choice is saving the serial number. In the new Europa series banknotes, the serial number is composed of 2 letters and 10 digits. Theoretically, 10 bits are needed for storing the two letters, but the first letter can assume only some fixed values, as it indicates the country responsible for printing the note. Therefore, the possible combinations of the two letters can be stored in 9 bits. In addition, 34 bits are required for the 10 digits number.

Secondly, the position and slope of all fibers in each banknote is stored. The size of this information depends on the desired precision. The position of the fiber's centroids can be saved with a discretization of 2 mm. This threshold simplifies the implementation of the proposed approach, by allowing some flexibility in the acquisition and analysis of the image. At the same time, it guarantees the unique identification of all existing banknotes, as proved hereinafter. A €50 banknote measures 140 mm x 77 mm; with the considered precision there are 70 different positions in the X axis and 39 positions in the Y axis. The coordinates are saved as a raster: there are P = 2,730 different positions, which can be encoded using 12 bits.

The slope angle can be any real value in the interval [0°, 360°], but there are a couple of advantages in discretizing that value. First, the amount of memory dramatically decreases when storing an integer value instead of a real one. Secondly, using discretized values lowers the precision required in detecting the slope angle: measuring the angle several times can lead to slightly different results, for example because the banknote is not always positioned in the same exact way, but these small differences can then be absorbed in the larger discretization error. On the other hand, a large discretization error can smooth the difference between the measured angles, so a proper trade-off is desirable. The proposed encoding uses 4 bits for saving the slope of a fiber: this amount guarantees a good resolution and significantly relaxes the memory constraints. By using 4 bits, the slope angle is discretized into 16 different values, each one covering $\pi/32\,\mathrm{rad} = 22.5°$. This range is approximated to 24 degrees in order to work with a convenient value.

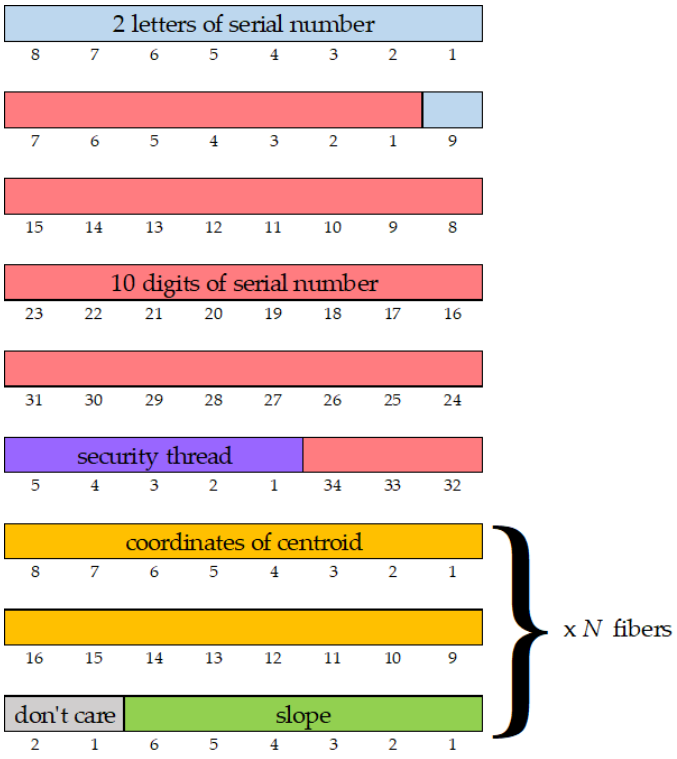


Fig. 5. Proposed encoding scheme, with bit size for each field. N is the number of fibers found in the banknote.

Thus the total number of values for the slope angle is A = 15. There is one probability out of 15 that two fibers at the same position are considered identical because they have the same slope; however this event is still not critical because the banknotes can be distinguished thanks to the position and orientation of the other fibers.

As discussed in Section 4.3, the security thread is detected more easily than the fibers, so a higher precision for its position can be used, e.g., 0.5 mm. However, it should be noted that this position varies within a short interval, approximately one eighth of the banknote length. So 5 bits are sufficient for storing its relative position.

As summarized in Fig. 5, the total amount of memory required for a banknote is 6 + 2·N bytes, where N is the number of fibers found in the banknote. By assuming that N = 20 fibers are found on average, the memory amount is 46 bytes. Nowadays, the total estimate of euro banknotes circulating is about 27 billions [30]. Consequently, the total memory that should be allocated to store the actual circulating banknotes is about 1.2 TB.

As a basis for comparison, the memory requirement of the proposed encoding is compared with another solution for saving the positions of the fibers [24], [25]. Here, the ultraviolet image of the banknote is divided into cells of 32 × 32 pixels. A binary value is associated to each cell: 1 means that the cell contains a part or the whole fiber; 0 means that no fibers are found inside the cell. The image of a €50 banknote is saved with dimensions of 1824 x 3392 pixels, which correspond to 57 x 106 cells [24]. Overall, there are 6042 cells: since each one carries one bit of information, the memory required for storing the fibers data in a €50 banknote is 756 byte. A grid with larger rows and columns can be used, dividing the banknote in 16 x 32 cells [25]. In that case the required memory for one banknote is 64 bytes, which corresponds to an increment of 40% with respect to the proposed encoding.

The proposed encoding is sufficient for uniquely identifying all existing banknotes. In fact, as a first approximation, let us suppose that the number of fibers is the same for each banknote. One end point of a fiber can be located in any position, and there are no preferred angles for the fiber slope. The number of N-combinations from the set of $N \cdot P \cdot A$ possible values is equal to a binomial coefficient:

$$C_{N \cdot P \cdot A, N} = \binom{N \cdot P \cdot A}{N}. \tag{2}$$

With the proposed encoding, and assuming N = 20, $C_{N \cdot P \cdot A, N} \sim$ 7.57e99, which is 89 orders of magnitude higher than the number of euro banknotes in circulation. This gap allows a more robust authentication procedure, as described in Section 6.

6 Probability of Misclassification

The methods for currency recognition and authentication surveyed in Section 2 are based on the assumption that it is extremely difficult for counterfeiters to accurately replicate some features of the banknote, such as fluorescence, patterns in visible or ultraviolet images, microprinting, watermark, etc. Therefore, it is not possible to determine the accuracy of these methods in recognizing genuine banknotes because it depends on the counterfeiters' ability, which is unknown. Also the methods that evaluate the presence of fibers [20], [21], [22], [23] can fall into error if the counterfeiters are able to insert fibers in false banknotes. Instead of the mere presence, the proposed anti-counterfeiting method analyzes the position of the fibers. Therefore, it is possible to compute the error rate, i.e., the probability of being misclassified when analyzing a banknote with fibers.

Given two banknotes A and B, containing N_A and N_B fibers respectively, we want to compute the probability that they share at least k fibers. A fiber is shared if the position of its centroid and the slope are the same in the two banknotes. In order to compute the probability, specific cases are evaluated initially, then a general formula is inferred.

First, two trivial cases can be recognized: the probability of sharing at least 0 fibers is 1, whereas the probability of sharing a number of fiber higher than min(N_A, N_B) is 0.

If N_A = 1, the probability that the fiber in A is located at the same place with the same slope as a fiber in B is equal to the ratio of N_B to all possible combinations of positions P and slope angles A (the values of P and A depends on the level of discretization, as discussed in Section 5). This probability can be expressed as a function of 4 parameters:

$$F(N_A = 1, k = 1, N_B, T) = \frac{N_B}{T} \tag{3}$$

where $T = P \cdot A$.

If N_A = 2, A and B share at least one fiber is one of the following events occurs:

- A shares its first fiber with B, but not the second one
- A shares both fibers with B

- A shares its second fiber with B, but not the first one.

The probability of the three events are added as follows:

$$F(N_A=2,k=1,N_B,T)=\frac{N_B}{T}\cdot\left(1-\frac{N_B-1}{T-1}\right)+ \\ +\frac{N_B}{T}\cdot\frac{N_B-1}{T-1}+\left(1-\frac{N_B}{T}\right)\cdot\frac{N_B}{T-1}= \\ =\frac{N_B}{T}+\left(1-\frac{N_B}{T}\right)\cdot\frac{N_B}{T-1}\,. \quad (4)$$

When computing the probability that the second fiber in A appears in B, the number of combinations of positions and slope angles is decremented by 1 because the location of the first fiber in A is excluded. It can be noted that with N_A = 2 the probability of sharing at least one fiber corresponds to the sum of two terms: the probability that the first fiber in A appears in B (as computed in (3) with N_A = 1), and the probability that the previous event does not occur, multiplied the probability that the second fiber in A appears in B.

The probability that A and B share two fibers is obtained by multiplying the probability of the two events:

$$F(N_A=2,k=2,N_B,T)=\frac{N_B}{T}\cdot\frac{N_B-1}{T-1}\,. \quad (5)$$

If N_A = 3, the probability that A and B share at least one fiber is obtained by adding to (4) the probability that neither the first or the second fiber of A appears in B, multiplied by the probability that the third fiber in A appears also in B:

$$F(N_A=3,k=1,N_B,T)=\frac{N_B}{T}+\left(1-\frac{N_B}{T}\right)\cdot\frac{N_B}{T-1}+ \\ +\left[1-\frac{N_B}{T}-\left(1-\frac{N_B}{T}\right)\cdot\frac{N_B}{T-1}\right]\cdot\frac{N_B}{T-2}\,. \quad (6)$$

The probability that A and B share at least two fibers is obtained as a sum of two terms:

- the probability that A and B share the first fiber and another one between the two others
- the probability that A and B do not share the first fiber, multiplied by the probability that they share the second and third fiber

$$F(N_A=3,k=2,N_B,T)=\frac{N_B}{T}\cdot\left[\frac{N_B-1}{T-1}+ \\ +\left(1-\frac{N_B-1}{T-1}\right)\cdot\frac{N_B-1}{T-2}\right]+ \\ +\left(1-\frac{N_B}{T}\right)\cdot\frac{N_B}{T-1}\cdot\frac{N_B-1}{T-2}\,. \quad (7)$$

The probability that A and B share three fibers corresponds to the probability of three events happening at the same time:

$$F(N_A=3,k=3,N_B,T)=\frac{N_B}{T}\cdot\frac{N_B-1}{T-1}\cdot\frac{N_B-2}{T-2}\,. \quad (8)$$

TABLE 1
Theoretical and simulated probability of misclassification.
N_A = 5, N_B = 5, T = 100, M = 500.

k	probability according to (10)	statistics from simulations	percent error
1	1.0	1.0	0.0
2	0.9999311	0.9999271	0.0004 %
3	0.2590195	0.2589061	0.0438 %
4	0.0031562	0.0031495	0.2133 %
5	0.0000066	0.0000067	0.8856 %

The probability that A and B share at least k fibers can be obtained by induction from the previous equations and by including the two trivial cases:

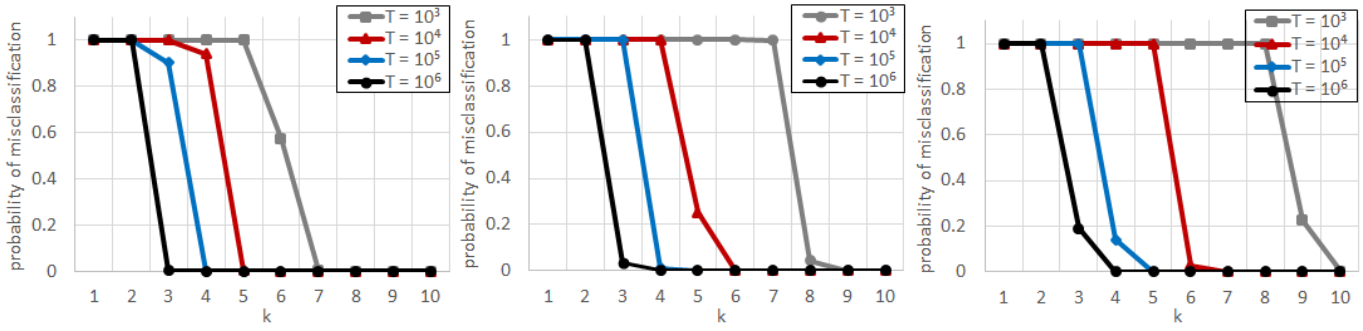
$$F(N_A,k,N_B,T)= \\ =\begin{cases}0 & \text{if } k>\min(N_A,N_B)\\ 1 & \text{if } k=0\\ \frac{N_B}{T}F(N_A-1,k-1,N_B-1,T-1)+ & \\ +\left(1-\frac{N_B}{T}\right)F(N_A-1,k,N_B,T-1) & \text{otherwise}\end{cases} \quad (9)$$

In the proposed approach, two banknotes are recognized as different if they share less than k fibers. The probability that a banknote A containing N_A fibers is not considered equal to another banknote B with N_B fibers is $1-F(N_A,k,N_B,T)$. The probability of not recognizing a false banknote, i.e., the probability that a false banknote shares at least k fibers with another one out of M banknotes, is estimated by using the simplified assumption that every other banknote contains the same number of fibers N_B:

$$P(\text{misclassification})=1-(1-F(N_A,k,N_B,T))^M\,. \quad (10)$$

The correctness of (10) has been confirmed by means of simulations, with the following setting: N_A = 5, N_B = 5, T = 100, M = 500. These values are considerably lower than real ones, but here the goal is to validate the theoretical formula. In fact, such low values were chosen in order to accelerate the execution of simulations. Consequently, statistics were collected from 10^7 randomly generated cases: this huge number of repetitions reduces the statistical error. As pointed out in Table 1, (10) well matches with the simulation results: the percent error, which is computed as $\frac{|simulation-theoretical|}{simulation}\cdot 100$, is negligible.

Fig. 6 plots the probability of not recognizing a false banknote according to (10). Three scenarios are considered: the number of fibers detected in the false banknote and in all the genuine ones is assumed constant and equal to 10, 15, 20 respectively. The amount of genuine banknotes is set equal to M = 27 billions, as estimated at the time of writing [30]. The number of fibers that must be checked in the currency authentication process depends on the adopted precision, i.e., the discretization of coordinates and slope angle. For example, if every banknote contains 15 fibers, and $T=10^5$ different combinations of positions and slope angles are considered, then the probability that a false banknote shares more than 4 fibers with any genuine ones is zero. This low threshold increases the fault tolerance of the proposed approach: the wrong detection of some



(a) $N_A = N_B$ = 10 fibers (b) $N_A = N_B$ = 15 fibers (c) $N_A = N_B$ = 20 fibers

Fig. 6. Probability that banknote A shares at least k fibers with any banknote B of 27 billions banknotes, depending on number of fibers $N_A = N_B$ detected in every banknote, and amount T of distinct positions and slopes of fibers.

fibers, due to implementation issues, banknote wear, external conditions, etc., does not affect the outcome of the classification. The encoding presented in Section 5 supports P = 2,730 different positions and A = 15 different slope angles: therefore $T = P \cdot A$ = 40,950 different combinations for the fibers placement are considered. As shown in Fig. 6, if every banknote has 20 fibers, then a banknote is classified as genuine if a match of at least 6 fibers is found.

The theoretical result proves the higher robustness of the proposed approach with respect to the other previous anti-counterfeiting techniques based on the fibers' position [24], [25]. In this context, the robustness is a measure of false negatives (i.e., genuine banknotes recognized as false), which can be due both to external causes (i.e., not concerning the anti-counterfeiting method) and internal causes. In fact, banknotes may be creased, got dirty or worn-out due to their frequent use: as a consequence, some fibers in the newly printed currency may be not detected any more when the banknote gets consumed, or, vice versa, a flaw in a worn-out banknote may be incorrectly recognized as a fiber. Moreover, different implementations (at both software and hardware level) of the fiber recognition process and different working conditions (e.g., brightness) may lead to different results, with a variable sensibility in recognizing short or faint fibers. In previous techniques [24], [25], the information on the fibers is stored in a matrix: each cell of the matrix contains a binary value indicating the presence or the absence of a fiber. All cells are compared to the benchmark through the exclusive OR operator. The variability in the fiber recognition is taken into account by admitting 1% of different cells: this threshold was empirically set. On the contrary, the theoretical analysis in this section proves that relatively few fibers have to be exactly recognized in order to assess the authenticity of a banknote. For example, recognizing at least 6 out of 20 fibers means that, even if 70% of the fibers are not correctly detected, the banknote can still be authenticated. That exceptionally higher threshold reveals the robustness of the proposed solution: constraints on the banknote conditions and on the implementation of the authentication process can be relaxed.

7 Results

The proposed anti-counterfeiting method is validated with respect to the proposed application scenarios. In particular, by means of a demonstrator, it is shown that the main characteristics required in all proposed scenarios are feasible.

Whereas encoding, by means of SHA256 and/or public/private key, can be considered feasible (given a reasonable computing power, such as CPUs installed in smartphones) other points have to be demonstrated. In particular, in all proposed scenarios it is mandatory to guarantee that:

- the total authentication time is lower than 2 seconds;
- the demonstrator can be built with an embedded system, in order to be used easily by a retailer.

For verifying such requests we have built a software able to perform the most demanding part, i.e., fibers' recognition. 25 banknotes of €50 Series 2 have been digitized by means of ultraviolet Wood transmitted light. Lamp is an ultraviolet SLT 26W BLB (220-240V), emitting light at 370 nm. All photos have been taken with an Olympus OM-D M10II with a Zeiss Makro Planar f2,8; 1/1.3s @f2, 8-200 ISO. Banknotes have been put in such a way that the serial number is visible.

Transmitted light has been used, differently than in other proposed methods, because fibers are inside the paper and can be seen on one side only in reflection. In transmission it is easier to see all (or almost all) fibers. One millimeter of banknote corresponds to 30.4 pixels: this guarantees a good level of details in the banknotes images. Flat field has not been applied, since light appears very well diffused. Demosaicing has been done by means of the Aliasing Minimization and Zipper Elimination (AMaZE) algorithm [31].

Fig. 7 displays the position of all fibers and security threads in the sample of 25 banknotes. When composing the chart, the results of the developed demonstrator were manually verified, collecting 935 fibers overall. In fact, it should be noted that some fibers that can be detected by looking the ultraviolet image of a banknote with the naked eye are not automatically recognized by the demonstrator. Possible reasons are short length or low brightness of the fiber, or similarity to the green background. It would be possible to adjust the thresholds adopted by the software in order to recognizing more fibers, but benefits would be limited. In fact, the important requirement is the correct recognition of few fibers: other undetected fibers, as well as wrongly recognized ones, do not affect the reliability of the authentication, as discussed in Section 6.

Circles in Fig. 7 correspond to the centroids of fibers. In the proposed anti-counterfeiting approach, the distinctive-

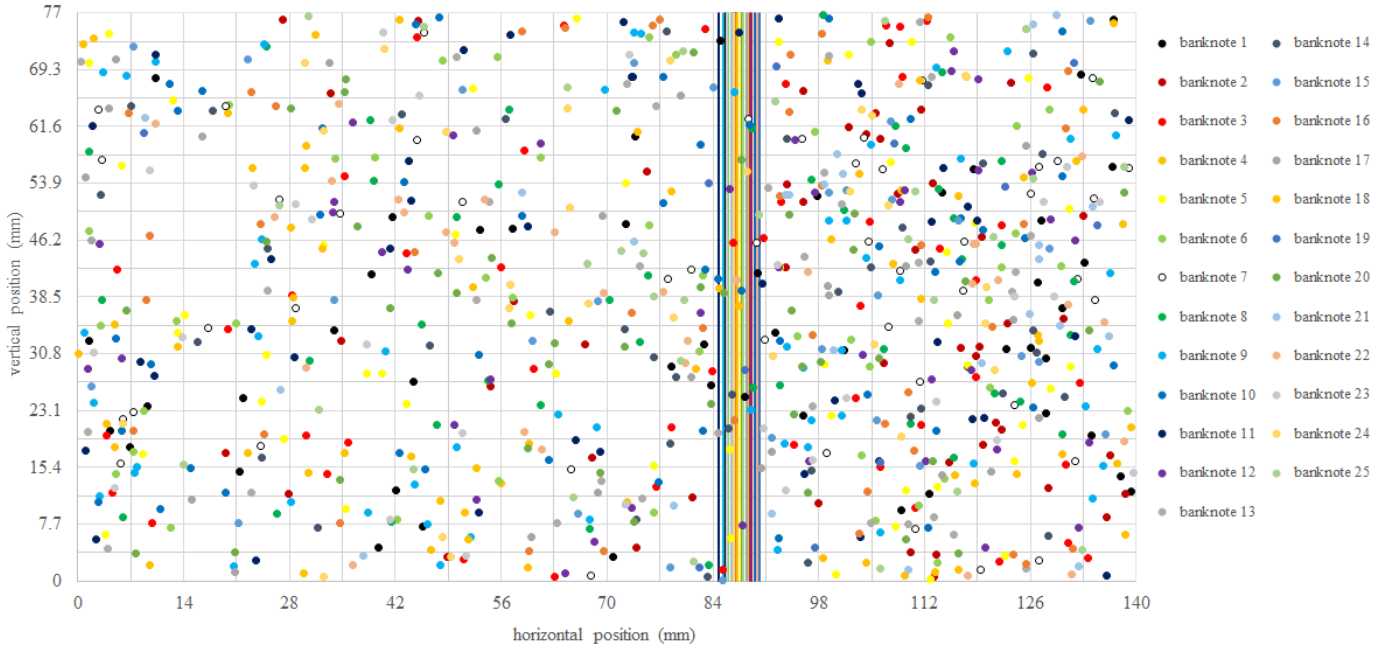


Fig. 7. Positions of fibers and security threads in the analyzed banknotes.

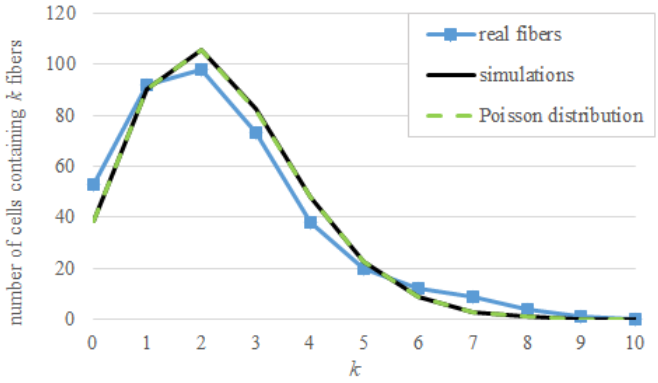
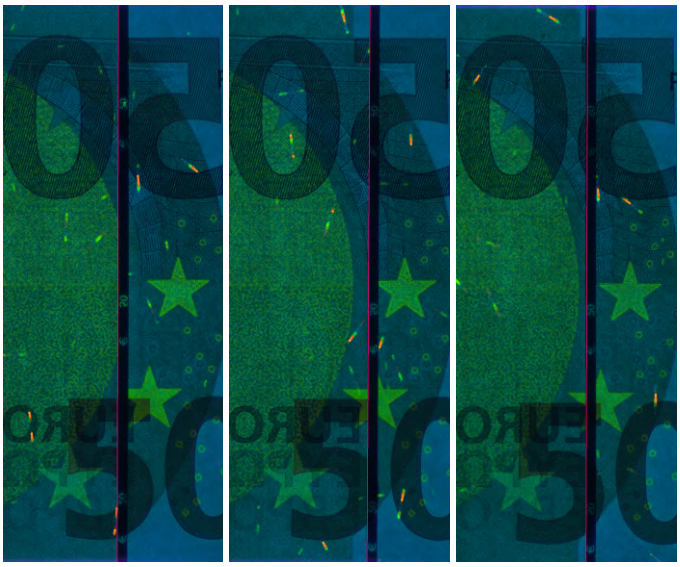


Fig. 8. Distributions of fibers in analyzed banknotes and in simulations.

ness of the fibers for identifying banknotes is based on their random positions, like the signs in human fingerprint. In order to verify that hypothesis, the plot area in Fig. 7 was split into a grid of 20x20 cells: each cell measures 7 x 3.85 mm. Then, the number of fibers in each cell was counted. As a comparison, a program that randomly deploys 935 points (as many as the fibers in the sample) in a 140 x 77 mm area was executed 10,000 times and the average statistics on the number of points in each cell were collected. As shown in Fig. 8, the simulation data follow a Poisson distribution, with mean equal to 935 / 400 = 2.3375. This behavior is consistent with the distribution of fingerprint minutiae [32]. The empirical data match well with the distribution obtained from simulations: slight differences can be explained with (1) statistical errors due to the low number of real fibers compared with the amount of points in the simulations (which is 10,000 times greater); (2) some areas where fibers are not visible, e.g., inside the female portrait and the three black boxes above and below (as can be noted in Fig. 3).

TABLE 2
Statistics about the position of the security thread (in pixel)

minimum	maximum	average	standard deviation
2545	2703	2624.2	41.5



(a) banknote 1 (b) banknote 3 (c) banknote 8

Fig. 9. Detail of three different €50 banknotes. The position of the security thread, which is highlighted with a red line, varies within a range of a few millimeters.

Most of the lines representing the security threads in Fig. 7 do not overlap: since differences are appreciable, it is worth to include also this information in the characterization of the banknote, as proposed in the encoding described in Section 5. Some statistics about the position of

TABLE 3
Statistics about execution time (ms) for 8 real banknotes

banknote	minimum	maximum	average	standard deviation
banknote 1	630	1249	649.8	21.6
banknote 2	635	1005	652.0	13.8
banknote 3	634	828	651.7	10.2
banknote 4	629	1012	646.6	14.3
banknote 5	636	885	651.1	9.7
banknote 6	636	1042	652.0	15.1
banknote 7	636	1183	651.9	18.5
banknote 8	600	1117	616.1	16.5

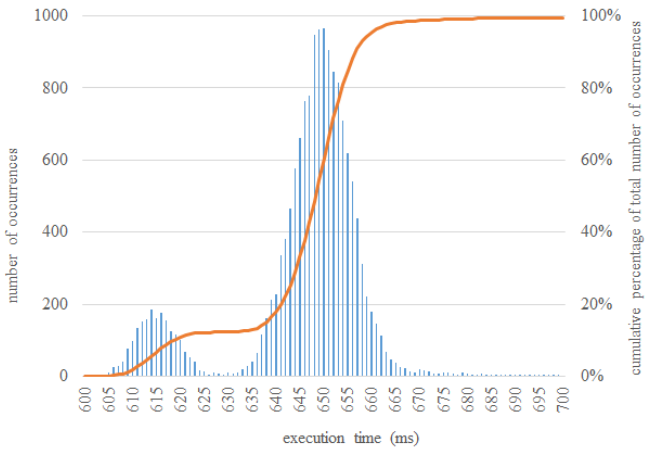


Fig. 10. Number of executions completed in a given amount of time for 8 real banknotes.

TABLE 4
Statistics about execution time (ms) for 8 fake banknotes

banknote	minimum	maximum	average	standard deviation
banknote 1	465	944	474.6	22.3
banknote 2	463	1543	475.9	33.2
banknote 3	466	1402	477.5	35.4
banknote 4	477	638	490.1	10.5
banknote 5	463	1262	476.5	42.8
banknote 6	466	559	474.9	9.5
banknote 7	465	592	474.6	10.4
banknote 8	469	724	479.0	10.9

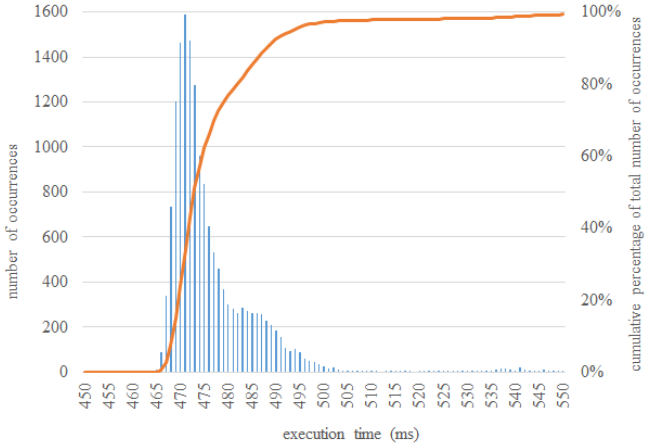


Fig. 11. Number of executions completed in a given amount of time for 8 fake banknotes.

the security thread, referring to the x-coordinate of the left-most pixel, are listed in Table 2. The interval of the positions is about 150 pixels, which corresponds to about 5 mm in the real banknote. According to the proposed encoding, in the considered sample there are up to 10 distinct values for the positions of the security thread, since a precision of 0.5 mm is adopted. Therefore, 5 bits for storing this information, as summarized in Fig. 5, are surely enough. The variability of the position of the security thread inside the analyzed banknotes can be appreciated in Fig. 9.

In order to collect statistics about the time required for the banknote authentication, a subset of 8 banknotes was analyzed 2,000 times by the developed demonstrator. The software runs on a Windows 10 desktop PC, with an Intel Xeon CPU E3-1245 v5 at 3.50 GHz and 32 GB or RAM. The main information collected during this experiments is reported in Table 3. The identification of fibers and security thread requires between 0.6 and 1.25 s: the proposed approach is suitable for the scenarios considered in Section 3, as the timing constraint of 2 s is always met. The average identification time is about 0.65 s; banknote 8 is an exception as it is processed faster (0.62 s on average). The low standard deviation suggests that most of the executions are close to the average timing. This is confirmed in Fig. 10, which plots the number of executions performed in a certain time, with a granularity of 1 ms. In fact, there is a peak around 650 ms, and a secondary peak around 615 ms, which is due to the analyses of banknote 8. Each point of the orange line in Fig. 10 indicates the percentage of software executions completed within the time indicated at the corresponding point on the x-axis. It is important to note that 99% of trials conclude within 675 ms, so values higher than 1 s, such as the maximum values listed in Table 3, are outliers.

Another experiment was performed in order to evaluate the performance of the demonstrator in presence of fake or worn-out banknotes. The 8 banknotes of the previous experiment were digitally edited: only a pair of fibers was left in each of them. The obtained images may resemble fake banknotes, reflecting in this way the difficulty of counterfeiters in reproducing fibers. Similarly, in this way also the effect of wear is simulated, as it can prevent the recognition of fibers in a genuine banknote. Table 4 and Fig. 11 report the statistics about the execution time of the demonstrator after 2,000 analyses of the 8 fake banknotes. It can be noted that the execution time is usually lower than in the previous test: the average time is 478 ms and the mode is 471 ms. The cumulative percentage of the total number of occurrences shown in Fig. 11 reveals that 99% of the analyses ended within 545 ms. It can be concluded that the lack of fibers does not penalize the evaluation of the banknote: on the contrary, the authentication of the banknote is quicker because there are few elements to be considered.

8 Conclusion

Colored fibers are security features already present in many currencies, such as euro banknotes. They are visible only when illuminated with ultraviolet light, so their presence is often manually checked with an ultraviolet lamp. However,

this check does not assure the genuineness of the banknote. The random position of fibers inside the banknote has been exploited in this paper in order to implement a method for unequivocally identifying the banknotes. A software, which was developed using OpenCV, recognizes fibers depending on their positions and slope. Furthermore, it recognizes the position of the security thread, which slightly varies from one banknote to another. The information detected by the software is unique for every banknote. Genuine banknotes can be listed with their distinctive features when printed; during the check phase, banknotes not present in the list are immediately classified as fake.

ACKNOWLEDGMENTS

The authors thank Andrea Gualco and Pietro Inglese for their help in the implementation and testing phases.

REFERENCES

[1] A. B. Centeno, O. R. Terrades, J. L. Canet, and C. C. Morales, "Identity document and banknote security forensics: a survey," *arXiv preprint arXiv:1910.08993*, 2019.
[2] D. Schaps, *The invention of coinage and the monetization of ancient Greece*. University of Michigan Press, 2010.
[3] H. de Heij, "Innovative approaches to the selection of banknote security features," in *Optical Security and Counterfeit Deterrence*, San Francisco USA, January 2010.
[4] H. de Heij, L. A. DiNunzio, and O. Strube, "Comparence EUR-USD banknotes," in *Banknote 2003*, Washington DC, USA, 2–5 February 2003.
[5] H. de Heij, "Occasional studies," 2007.
[6] L. Cozzella, C. Simonetti, and G. Schirripa Spagnolo, "Is it possible to use biometric techniques as authentication solution for objects? Biometry vs. hylemetry," in *5th International Symposium on Communications Control and Signal Processing*. IEEE, 2012, pp. 1–6.
[7] European Central Bank, "ECB to redesign euro banknotes by 2024," https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr211206~a9e0ba2198.en.html, accessed: 2022-04-04.
[8] T. D. Pham, C. Park, D. T. Nguyen, G. Batchuluun, and K. R. Park, "Deep learning-based fake-banknote detection for the visually impaired people using visible-light images captured by smartphone cameras," *IEEE Access*, vol. 8, pp. 63 144–63 161, 2020.
[9] S. Wang, E. Toreini, and F. Hao, "Anti-counterfeiting for polymer banknotes based on polymer substrate fingerprinting," *IEEE Trans. on Information Forensics and Security*, vol. 16, pp. 2823–2835, 2021.
[10] C. Park, S. W. Cho, N. R. Baek, J. Choi, and K. R. Park, "Deep feature-based three-stage detection of banknotes and coins for assisting visually impaired people," *IEEE Access*, vol. 8, pp. 184 598–184 613, 2020.
[11] K. Thierauf, "Device and method for verifying the authenticity of banknotes," Jul. 19 2005, US Patent 6918482.
[12] T.-Y. Chien, S.-P. Chan, and Y.-P. Hsu, "Banknote acceptor using ultraviolet ray for verification," Aug. 2006, US Patent 11 501108.
[13] J. G. Hopwood, L. J. Baron, L. J. Tenenbaum, S. P. Raphael, and P. R. Skipper, "Detection of counterfeit objects, for instance counterfeit banknotes," Jul. 6 1999, US Patent 5918960.
[14] B.-K. Kim, E.-C. Lee, B.-M. Suhng, D.-Y. Ryu, and W.-H. Lee, "Feature extraction using FFT for banknotes recognition in a variety of lighting conditions," in *13th International Conference on Control, Automation and Systems (ICCAS)*. IEEE, 2013, pp. 698–700.
[15] S.-H. Chae, J. K. Kim, and S. B. Pan, "A study on the Korean banknote recognition using RGB and UV information," *Communication and Networking*, pp. 477–484, 2009.
[16] K.-H. Lee and T.-H. Park, "Image segmentation of UV pattern for automatic paper-money inspection," in *11th International Conference on Control Automation Robotics & Vision (ICARCV)*. IEEE, 2010, pp. 1175–1180.
[17] A. P. Pujiputra, H. Kusuma, and T. A. Sardjono, "Ultraviolet rupiah currency image recognition using Gabor wavelet," in *International Seminar on Intelligent Technology and Its Applications (ISITIA)*. IEEE, 2018, pp. 299–303.
[18] Z. Dinku and K. Raimond, "Counterfeit currency identification system-a case study on Ethiopian Birr note," *Zede Journal*, vol. 26, pp. 73–78, 2009.
[19] A. Roy, B. Halder, U. Garain, and D. S. Doermann, "Machine-assisted authentication of paper currency: an experiment on Indian banknotes," *International Journal on Document Analysis and Recognition (IJDAR)*, vol. 18, no. 3, pp. 271–285, 2015.
[20] Z. Ahmed, S. Yasmin, M. N. Islam, and R. U. Ahmed, "Image processing based feature extraction of Bangladeshi banknotes," in *8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. IEEE, 2014, pp. 1–8.
[21] A. Zarin and J. Uddin, "A hybrid fake banknote detection model using OCR, face recognition and hough features," in *Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 91–95.
[22] C. Chang, T. Yu, and H. Yen, "Paper currency verification with support vector machines," in *3rd Int. Conf. on Signal-Image Technologies and Internet-Based System (SITIS)*. IEEE, 2007, pp. 860–865.
[23] B. Halder, R. Darbar, U. Garain, and A. Mondal, "Analysis of fluorescent paper pulps for detecting counterfeit Indian paper money," in *International Conference on Information Systems Security*. Springer, 2014, pp. 411–424.
[24] G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, "Banknote security using a biometric-like technique: a hylemetric approach," *Measurement Science and Technology*, vol. 21, no. 5, pp. 1–8, 2010.
[25] ——, "Currency verification by a 2D infrared barcode," *Measurement Science and Technology*, vol. 21, no. 10, pp. 1–5, 2010.
[26] F. van der Horst, J. Miedema, and M. van der Woude., "Perception of public security features on euro banknotes. a qualitative survey on confidence and authenticity," *IBDA-Insight*, no. 13, May 2017.
[27] F. V. der Horst, M. Eschelbach, S. Sieber, and J. Miedema, "Does banknote quality affect counterfeit detection? Experimental evidence from Germany and the Netherlands," in *Bank Working Paper No. 499*, 2016.
[28] H. de Heij, *The Banknote Designer and the Banknote Design Manager. Who does what?*, 1st ed. International Banknote Designers Association (IBDA) in cooperation with De Nederlandsche Bank, 2017.
[29] R. Laganière, *OpenCV 2 computer vision application programming cookbook*. Packt Publishing, 2011.
[30] European Central Bank, "Banknotes and coins circulation," https://www.ecb.europa.eu/stats/policy_and_exchange_rates/banknotes+coins/circulation/html/index.en.html, accessed: 2022-04-04.
[31] A. Forsey and S. Gungor, "Demosaicing images from colour cameras for digital image correlation," *Optics and Lasers in Engineering*, vol. 86, pp. 20–28, 2016.
[32] J. Chen and Y.-S. Moon, "A statistical study on the fingerprint minutiae distribution," in *IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, vol. 2, 2006, pp. 169–172.

Renato Ferrero (M'13, SM'20) received the M.S. degree in Computer Engineering in 2004 and the Ph.D. degree in Computer and System Engineering in 2012, both from Politecnico di Torino, Italy. He is currently an Associate Professor at the Dipartimento di Automatica e Informatica of Politecnico di Torino. His research interests include ubiquitous computing, wireless sensor networks and RFID systems.

Bartolomeo Montrucchio (M'02, SM'21) received the M.S. degree in electronic engineering and the Ph.D. degree in computer engineering from the Politecnico di Torino, in 1998, and 2002. He is currently a Full Professor of Computer Engineering with the Dipartimento di Automatica e Informatica, Politecnico di Torino. His current research interests include image analysis and synthesis techniques, scientific visualization, sensor networks, RFIDs and quantum computing.