Optical detection of random features for high security applications

T.Haist and H.J. Tiziani
Institut für Technische Optik, University of Stuttgart

***Abstract*— Optical detection of random features in combination with digital signatures based on public key codes in order to recognise counterfeit objects will be discussed. Without applying expensive production techniques objects are protected against counterfeiting. Verification is done offline by optical means without a central authority. The method is applied for protecting banknotes. Experimental results for this application are presented. The method is also applicable for identity verification of a credit– or chip–card holder.**

***Index Terms*— security, fraud, optical detection, correlation, paper, digital signatures**

I. Introduction

HIGH security against counterfeit is achieved usually by complex methods too expensive or not accessible for counterfeiters. Modern examples are credit cards with phase masks[1] , banknotes with holograms[2] and smart identity cards or keys. Unfortunately these methods have some serious drawbacks: 1. technological progress might simplify copying in future, 2. expensive production techniques may only suitable for mass products like credit cards or banknotes, 3. professional fraudsters are hard to scare away by cost intensive reproduction.

In order to avoid these problems, random features can be used to obtain security against counterfeiting[3], [4], [5], [6]. These features have to be extremely complicated and therefore very hard, if not impossible, to copy. Important examples are the three–dimensional distribution of bubbles in transparent materials, the fibre structure of paper or surface profiles in connection with material properties. Microscopic features are especially interessting for security purposes because they are hard to copy.

Optical methods seem to be most suitable for the nondestructive detection of such features. After detection, the object features are digitally stored on the object itself.

By using digital signatures based on public key codes, only an authorised person is able to store the detected information.

As an example, we used this method in order to protect German banknotes against counterfeiting. Practical results obtained for this application are presented.

II. Method description

The method used for protecting a banknote against counterfeit is shown in figure 1. The fibre structure of a small region of the banknote is detected by using a video microscope and digitised with a frame grabber. After some basic image processing, the image is compressed and a digital signature using public key authentification, is appended. The result is processed with a fault-tolerant code. This code is directly printed onto the banknote. The coded image serves as a reference for the verification process.

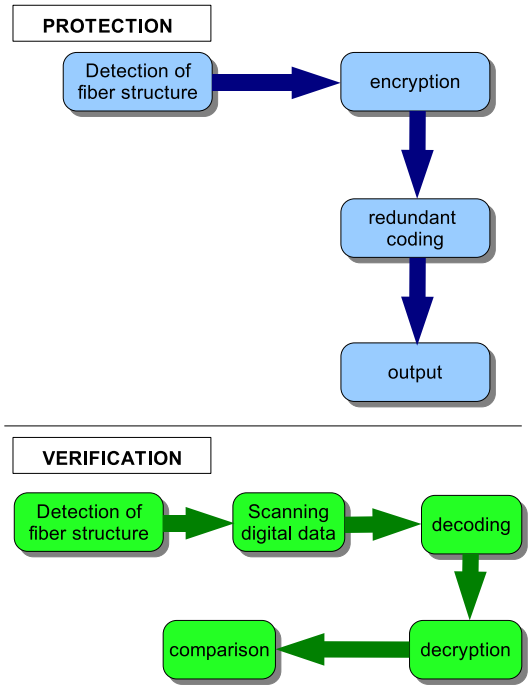


Fig. 1. Protection and verification of banknote

Verification of the banknote (see figure 1) is achieved by detecting the fibre structure and comparing it with the digitally stored reference image. The same setup as that of the coding procedure is used in order to detect the fibre structure. The coded reference image is read with a standard image scanner. After decoding, this reference image is compared to the fibre structure on the banknote. If the difference between both is above a threshold, we assume a counterfeit banknote.

The use of digital signatures is essential for the working of the method. These techniques (digital signatures are based on asymmetric codes) guarantee that only one central authority can produce the protected banknotes while everyone is able to verify them.

In 1995 Chu et al[7] and Vaidya[8] proposed the use of digital signatures in order to protect magnetic cards against fraud. Chu used “fuzzy bits”, a very inexpensive and therefore interessting approach. Unfortunately, copying such cards is still possible by using non–standard card readers. Vaidya based

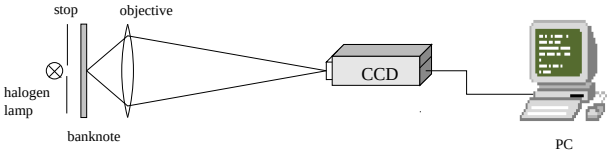


Fig. 2. Experimental setup for the detection of fibre structure

his method on “Watermark Magnetics” [1], a technology controlling the orientations of magnetic particles during production of the card. By using “sophisticated and secret production techniques” this method claims to manufacture magnetic cards which are “virtually impossible to copy”.

Our approach differs from these methods as we detect random features, which are already present on the object, by optical means. Therefore, high security without sophisticated and secret production techniques is achieved. Differences between our approach and the methods in refs [3], [4], [5] and [6] are the explicit use of digital signatures and the security features we use (the microscopic fibre structure of ordinary paper).

In the following, we give a detailed description of the different parts of the system and show experimental results for our application.

III. Detailed description and experimental results

A. Image acquisition

For the detection of the fibre structure we use a standard CCIR–CCD camera, an ITEX VFG frame grabber and a standard microscope objective (3.2 X, NA = 0.12). The banknote is illuminated by a 35 W halogen bulb. The setup is depicted in figure 2. Best contrast of the fibre structure was obtained by putting the illumination source about 1 cm behind the banknote (a German 5 DM banknote). A typical image obtained with this method is shown in figure 4.

Since we use one part of the grabbed image only, exact positioning of the banknote isn’t necessary. Orientation of the banknote should be controlled to about 1 degree.

B. Image processing and coding

The image processing performed is shown in figure 3: first, the region of interest within our image is extracted. In our example we choose the area within one half of the letter ’B’ of “Bundesbank” printed on the banknote resulting in a 180×200 pixel area with 8 bit gray scale. After edge–sharpening according to ref. [10] the histogram is equalised and smoothed with a simple 3×3 kernel (see figure 5). The image is stored using lossy JPEG compression (a standard platform independend image format) with 10 % quality and 20 % smoothing, resulting in about 2.86 KByte of data.

Of course we could further reduce the amount of data by using less pixels which unfortunately diminished the immunity against noise and local errors. In order to optimise performance, extensive statistical investigations concerning the optimal number of pixels for the application at hand are necessary.

[1]Watermark Magnetics is a registered trade mark of THORN EMI

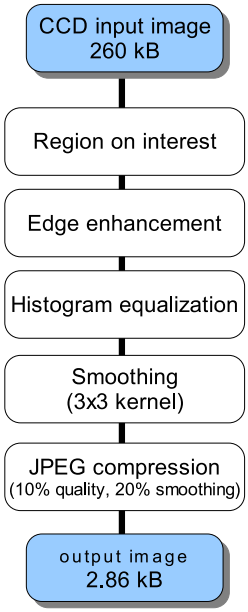


Fig. 3. Image processing

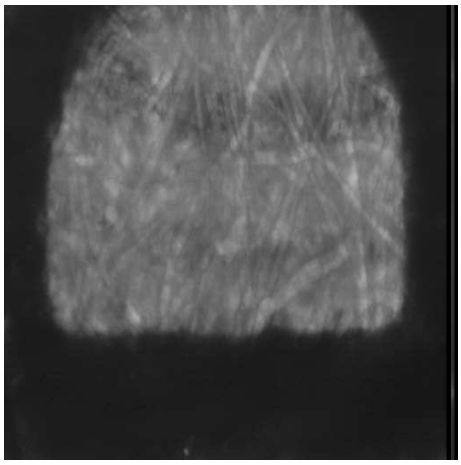


Fig. 4. Detected image

C. Coding

For the data (2.86 KByte) obtained by the lossy compression, a digital signature is generated. Various well known algorithms are available for this purpose. DSS (“Digital Signature Standard”[9]) and RSA authentification[11] are the most prominent examples. Typically, the data is processed with a one–way hash function (e.g. the MD5 or SHA-1 algorithm[12]) in order to generate a short description, the so called “message digest”. This message digest is processed with a public key authentification algorithm resulting in the digital signature which is appended to the data.

By using asymmetric public key codes, we achieve that it is possible for everyone to decrypt data using the public key while encryption with this public key remains impossible.

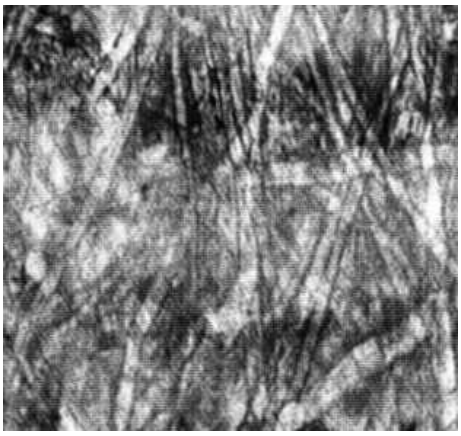
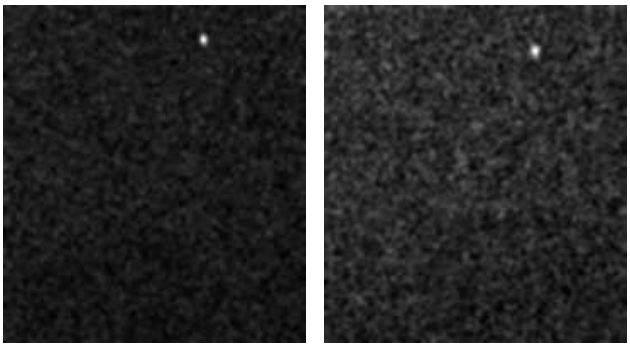


Fig. 5. Detected image after image processing



a.) b.)

Fig. 6. Correlation of reference with a.) the same banknote without repositioning , b.) the same banknote but with repositioning

The institution manufacturing the banknotes therefore creates a private encryption key and the corresponding public key for decryption. The encryption key is now used to create the digital signatures. Using the public key, everyone can decode the signatures and verify their authenticity. Since a falsifier has no access to the private key, he isn't able to create digital signatures for the fibre structures which he detected on his counterfeit banknotes.

We use the RSA algorithm in connection with the MD5 hash function and a 1024 Bit key (used with the public domain software "pgp") for the generation of the digital signature. This results in a 60 bytes signature for our data files.

The image and its digital signature are coded afterwards in order to transform the binary output into a printable format (e.g. hex or bar codes). Because of dirt or damage, it is possible that part of the printed information is unreadable on the banknote. The coding should therefore insert redundancy in order to obtain error correction abilities[16]. A non-local distribution of information offers additional security against localised damage and dirt.

D. Output

Storage of information is simple for credit–, chip– or identity–cards. On credit– and chip–cards the data is stored by magnetic or electronic means. With banknotes, only the paper can be used for information storage. Therefore the coded information has to be printed onto the banknote using a high quality printer. Banknotes are fortunately large enough to store two compressed and coded images by using only a small part (7 %) of the available paper. We can print approximately 3250 detectable ASCII characters on an area of 5.0 cm^2 with a standard laser printer. The German 100 DM banknote has an area of 222 cm^2. Using a simple hamming(7,4) code we would have to store 5 KByte per image resulting in a toleratable bit error probability of 14 %.

Using two coded images means an additional redundancy which further reduces the problems associated with dirty or damaged banknotes.

The necessary storage capacity could be dramatically reduced if we would not store the complete bitmap but a high level description of the fibres. Of course, it is a difficult problem to automatically obtain such a description. Other security features like bubbles in plastic are easier to describe (3D coordinates of the bubbles).

E. Decoding

The coded reference image is read into the computer by the aid of an image scanner. Error correction and decoding is straightforward and only depends on the used code. Afterwards, the digital signature is checked with the public RSA key in order to verify the authenticity of the digital data.

F. Verification of detected image with coded reference image

The detected image is compared with the coded reference image. Different methods are possible. We use a non–linear binary correlator with some post-processing of the obtained output in order to achieve the necessary immunity against local errors and additional noise.

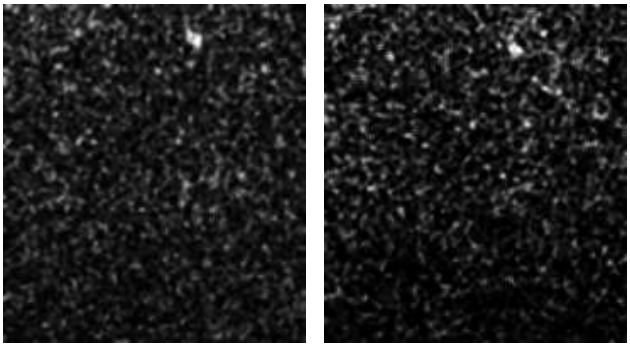
First we multiply the spectrum of the reference image with the complex conjugated spectrum of the detected image. The result is binarized and inverse Fourier transformed to obtain the correlation output. This correlation output is smoothed 2 times with a simple 3×3 kernel and normalised to 255 afterwards.

To avoid problems with the 0th order of the correlator, we shift the reference image by a fixed amount. Small deviations in the position of the banknote are not of concern since this only results in a corresponding shift of the correlation peak. The Fourier transforms are calculated electronically via the fast–Fourier–transform (FFT) algorithm with additional zero–padding. Acceleration is possible by using specialised electronic hardware, equipped with FFT chips. By storing not the reference image but rather its Fourier transform we can, of course, reduce the computational cost by about one third. For high-speed applications optical processing is necessary. SSDA algorithms[15] might be an interesting alternative to correlation methods with pure digital processing.

Figures 6, 7 and 8 show that easy detectable outputs with this rather simple method are achieved. The images in figure 6 correspond to the same banknote without and with repositioning. Figure 7 shows results for the same banknote with extreme wrinkles and with dirt and writings on the detected 'B'. The images in figure 8 depict results of correlation obtained with

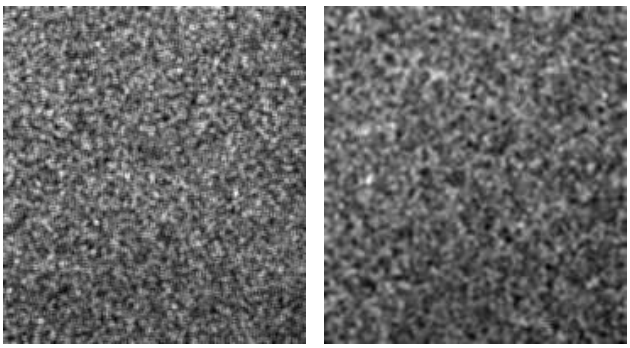
different other banknotes. We obtain detectable peaks at the expected positions with the original banknote whereas the counterfeit banknotes (in this case simply other banknotes) don't correlate at all. Further improvement is possible by using more sophisticated correlators. It should be especially advantageous to use (and store) optimised filters instead of Fourier transforms of the reference images. Optimised binary filters[14] would further reduce the necessary storage capacity.

Standard image processing techniques for the detection of simple fraud should additionally be used.



a.) b.)

Fig. 7. Correlation of reference with a.) wrinkled banknote, b.) with dirty banknote



a.) b.)

Fig. 8. Correlation of reference with different banknotes

IV. Summary and conclusions

We used the optical detection of random features in connection with public key authentification for protecting banknotes against counterfeiting. For this application experimental results are presented. Besides banknotes, the method can be used for credit– and chip–cards, checks, contracts, access control and identification systems, artworks, machine parts and a lot of other objects. For all these applications, most of the practical problems we were confronted with banknotes (dirt, wrinkle, low storage capacity) vanish. High security is obtained without expensive production techniques because the complicated features, used for verification, are already present on the object.

We want to point out, that instead of using random features of objects, we can also detect, code and store characteristics of persons who are authorised to use the objects. Possible examples of such characteristics are fingerprints, speech or retinal patterns, iris textures and faces. This is similar to a patent of Eastman Kodak obtained in 1994[13]: fingerprints or faces are stored on credit cards for verification of the correct card holder identity. Since symmetric codes are used, a central administration agency is needed. Offline verification is not possible and a lot of practical problems occur; it is expensive and seems not to be suitable for applications like world–wide ATMs. By using the proposed asymmetric public–key codes and random features, these problems can be avoided.

References

[1] B. Javidi, J.L. Horner: "Optical pattern recognition for validation and security verification", Optical Engineering 33, pg. 1752–1756 (1994)

[2] C.E. Chesak: "Holographic counterfeit protection", Optics Communications 115, pg. 429–436 (1995)

[3] R.N. Goldman: "Non–counterfeitable document system", US Patent 4785290 (1988) and US Patent 4663622 (1987)

[4] J. Samyn: "Method and apparatus for checking the authenticity of documents", US Patent 4820912 (1989)

[5] H. Hoshino, M. Yoda, I. Takeuchi, T. Kurihara: "Method and apparatus for checking objects to be checked for authenticity", US Patent 5473147

[6] R.L. van Renesse: "3DAS: A 3dimensional–structure authentification system", European Convention on Security and Detection 1995, IEE conference publication No. 408, pg. 45–49 (1995)

[7] M.C. Chu, L.L. Cheng, L.M. Cheng: "A novel magnetic card protection system", European Convention on Security and Detection 1995, IEE conference publication No. 408, pg. 207–211 (1995)

[8] A.W. Vaidya: "Keeping card data secure at low cost", European Convention on Security and Detection 1995, IEE conference publication No. 408, pg. 212–215 (1995)

[9] "The Digital Signature Standard proposed by NIST" and responses, Communications of the ACM 35(7), pg. 36..54 (1992)

[10] D.E. Knuth: "Digital halftones by dot diffusion", ACM Transaction on Graphics Vol. 6(4), pg. 245–273(1987)

[11] R.L. Rivest, A. Shamir, L. Adleman: "A method for obtaining digital signatures and public–key cryptosystems", Communications of the ACM 21(2), pg. 120–126 (1978)

[12] B. Schneier: "One–way hash functions", Dr. Dobbs Journal, 9/91, pg. 148–150 (1991)

[13] L.A. Ray: "Method and apparatus for credit card verification", European Patent 0 612 040 (1994)

[14] M.S. Kim, M.R. Feldman, C.C. Guest: "Optimum encoding of binary phase–only filters with a simulated annealing algorithm", Optics Letters 14, pg. 545–547 (1989)

[15] D.I. Barnea, H.F. Silverman: "A Class of Algorithms for Fast Digital Image Registration", IEEE Transactions on Computers, Vol. C-21, pg. 179–186, (1972)

[16] P.M. Grant, C.F.N. Cowan, B. Mulgrew, J.H. Dipps: "Analogue and digital signal processing and coding", Chartwell–Bratt Studentlitteratur, pg. 217–246 (1989)