Certifying Authenticity via Fiber-Infused Paper

Yuqun Chen, M. Kivanç Mihçak, and Darko Kirovski
Microsoft Research

A certificate of authenticity (COA) is an inexpensive physical object that has a random unique structure with high cost of near-exact reproduction. An additional requirement is that the uniqueness of COA's random structure can be verified using an inexpensive device. Bauder was the first to propose COAs created as a randomized augmentation of a set of fibers into a transparent gluing material that randomly fixes once for all the position of the fibers within. In this paper, we propose a novel system for automated verification of fiber-based COAs and outline the key challenges in enabling high cost-efficiency of such a system. The key features of the new COA scanner are simplicity, reliability, lack of any moving components, and the ability to accurately identify exact positions of individual fibers infused in COA's containing paper. The latter feature significantly increases the forging cost compared to trivial implementations of a COA scanner.

Categories and Subject Descriptors: C.3 [**Special-purpose and Application-based Systems**]: Real-time and embedded systems; K.4.4 [**Computers and Society**]: Electronic Commerce

General Terms: Security, Economics

Additional Key Words and Phrases: certificates of authenticity, anti-piracy, counterfeit deterrence.

1. INTRODUCTION

Counterfeiting is as old as the human desire to create objects of value. For example, historians have identified counterfeit coins just as old as the corresponding originals. For most of them, by now age has scraped off the thin layer of silver or other, then precious, metals exposing an inexpensive base. Even then, there were examples of counterfeit coins netting a 600% instant profit to the counterfeiter [1]. Test cuts were likely to be the first counterfeit detection procedure – with an objective to test the purity of the inner structure of the coin. The appearance of counterfeit coins with already engraved fake test cuts initiated the cat-and-mouse game of counterfeiters with original manufacturers that has lasted to date [1]. Fake coins in ancient times have been so common that Pliny the Elder (23-79 AD) has mentioned that collection of fake coins was a popular hobby at the time. There were instances of fake coins fetching several times their face value! Historically, counterfeiting has been a devastating problem for any economy. The paper currency bills of the Ming dynasty (1368-1644) contained the following clause: "To counterfeit is death. The informant will receive 250 taels in silver and in addition the entire property of the criminal." The ease of counterfeiting has forced the Chinese to abolish paper money in 1450 for the forthcoming four centuries. Money was not the only target for pirates. For example, under an early English statute (1350), counterfeiting the king's seal was a grave crime against the state amounting to high treason and was punishable by death. Historically, if not addressed, the expectation for counterfeiting has been enormous. During the Civil War, one-third to one-half of the currency in circulation was counterfeit. At that time, approximately 1600 state banks designed and printed their own bills. Each bill carried a different design, making it difficult to detect counterfeit bills from the 7000 varieties of real bills.

It is hard to assess and quantify the market for counterfeit objects of value today. With the ease of marketing products on-line, it seems that selling counterfeit objects has never been easier – industries under attack include the software and hardware, the pharmaceutical, the entertainment, and the fashion industry. For example, according to a 2000 software piracy study by International Planning & Research Corp., software piracy resulted in the loss of 118,026 jobs in the United States, nearly $1.6 billion in tax revenues and $5.6 billion in wages.

1.1 Certificate of Authenticity

A certificate of authenticity (COA) is an inexpensively manufactured object which is expensive to near-exactly replicate. Commonly, it is physically attached to a product with an objective to vouch for its authenticity. Traditionally, a common requirement for a COA has been that its genuineness be easily ascertained by a consumer, typically through visual inspection. The very ease of use of this type of *human-verifiable COA* has turned out to be its Achilles' Heel: a counterfeiter only needs to replicate the visual effects of a genuine COA in order to fool untrained inspectors.

Adding highly delicate, machine-readable features to a COA can potentially make counterfeiting more difficult, as machine identification is more accurate and less prone to certain kinds of deceits. But one must be careful with the type of machine-readable features: it is far better to vary the features per individual COA instance and preferably the features cannot be easily scanned and printed. An unvarying micro feature, i.e., a fixed pattern of finely engraved shapes on a currency bill, could be replicated *en masse* once the counterfeiting party learns how to build the "feature-stamping" machine. The high capital investment in building this machine could be recuperated by the high quantity of counterfeit COAs it later produces. As an example, counterfeiters have been economically successful in forging *en masse* anti-counterfeiting holographic features, regardless of their sophistication. Given above considerations, the authors believe that a robust and cost-effective COA technology should have the following set of desirable properties:

—**Uniqueness**: each COA instance is of a unique structure that is markedly different from any other instances.

—**Multi-dimensionality**: the response from a single COA instance cannot be generated by a simple two- or one-dimensional object.

—**Secure Authentication**: the unique feature can securely authenticated, possibly via public-key cryptography, during times of validation.

—**Low Production Cost**: the cost of creating an original COA is small, relative to a desired level of security.

—**High Replication Cost**: the cost of exact or near-exact replication is several orders of magnitude higher than production cost.

—**Inexpensive Validation**: the cost of verifying the authenticity of a COA, both in dollar amount and in time, is small, again relative to a desired level of security.

In the remainder of this article, we describe the basic principles used to design a practical fiber-based COA technology that possesses above properties.

2. FIBER-BASED COA

We follow the idea that was first introduced by Bauder and Simmons at the Sandia National Labs [3; 4]. Each COA instance is created as a collection of fibers randomly positioned in an object using a transparent gluing material which permanently fixes fibers' positions [3; 4]. Readout of the random structure of a fiber-based COA can be performed in numerous ways using the following fact: if one end of a fiber is illuminated, the other end will also be lit as shown in Figure 1.

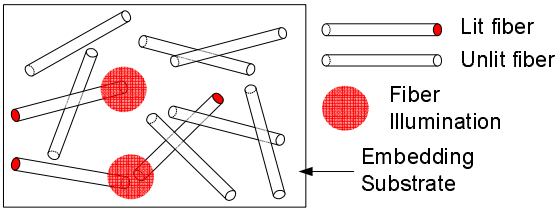

Fig. 1. A conceptual example of COA with randomly-placed, fixed-length fibers. Three fibers are "lit" by two spot illumination lights.

The key to counterfeit deterrence of a fiber-based COA lies in the fact that a strand of optical fiber conducts light between two distinct points. A collection of optical fibers are to be described in a dimensionality that is higher than that of a regular two-dimensional image. In the most general case where the fibers are of arbitrary length, this dimensionality is four as exactly four coordinate numbers are needed to describe each fiber: two for the x and y coordinates of each fiber tip. Even when the length of the fibers is fixed or varies within a small range, as is the case for most applications, the dimensionality is still equal to or greater than three.

This high dimensionality, coupled with the uniqueness of each randomly-generated fiber pattern, makes the proposed COAs drastically different from the typical anti-counterfeiting features. They are either two-dimensional, or unvarying, or both in nature [16]. Two-dimensional features are easily copied by the use of printers or special press-molding devices.

2.1 Related Work

Bauder was the first to propose the use of epoxy spray-painted surfaces as certificates of authenticity in the 1970s during the Cold War for weapons control verification purposes [3]. Once applied, the epoxy would create a random rough surface which would have a distinct reflective glow if light was shed from a particular angle. By taking a photograph of this illumination, Bauder's team would record a single COA instance. In the 1980s, Bauder and Simmons proposed randomly-embedded optical fibers as an counterfeit-deterrent feature for US banknote protection [4].

Only a few efforts have followed since Bauder's pioneering work. Church and Littman have worked on extraction of random optical-fiber patterns in the context of currency anti-counterfeiting [5; 9][1]. Most recently, Pappu created a class of

[1]Unfortunately, we have been unsuccessful in obtaining details about this work in order to make a meaningful comparison with ours. The date when it was conceived suggests strong differences.

physical one-way functions via speckle scattering [10]. He has focused on Gabor wavelets to produce short digests of the natural randomness collected from an optical phenomenon. His Ph.D. thesis also has a solid survey of the related but scarce work [10]. Finally, several industrial efforts have resulted in designs that mimic multidimensional certificates [11; 12; 13; 14; 15], however, none of them have responses that cannot be provably spoofed or generated by inexpensive two-dimensional structures.

3. SYSTEM DESCRIPTION

A COA instance is issued in the following way. First, a certain hard-to-replicate statistic of COA's unique structure (e.g., positions of the fibers) is extracted by a scanner. This unique "fiber signature" of a COA instance is then digitized and compressed into a bit string f. Next, f is concatenated to the associated product information g (e.g., product ID and expiration date) to form a combined bit string $w = f||g$. The combined bit string along with a signed hash of the combined bit string w is then appended to it to form a message $m = w||S(H(w))$. The hash function H is a cryptographically-strong algorithm such as SHA256 [8]. In order to guard against the possibility that a verifier may fall into the hands of the adversary, the signing function S is based on public-key cryptography [2; 6; 8; 17], so that the issuer signs $H(w)$ with his private key and the verifier validates the integrity of m using the public key. Finally, the message m is encoded directly on the COA using a barcode or RFID.

Verifying a COA instance involves the following steps. The verifier first scans the message $m = w||S(H(w))$ from the tag and verifies the integrity of w using the corresponding public key and $S(H(w))$. Once the integrity of w is ascertained, the original fiber statistics f and the product information g are extracted from w. The verifier proceeds to scan the fiber pattern in the COA, obtain a new reading of the fiber signature f', and compare it with f. If the level of similarity between f and f' exceeds a pre-defined threshold, the verifier declares the COA instance to be authentic; otherwise, counterfeit.

In order to counterfeit protected objects, an adversary needs to either:

(i) Compute the private key of the COA issuer so that she can sign any random fiber patterns that she creates. This attack can be made arbitrarily difficult by adjusting the length of the key used in S [17; 2; 6], or

(ii) Devise a manufacturing process that can exactly replicate an already signed COA instance – a task which is not infeasible but requires a high expense by the malicious party – the forging cost dictates the value that a single COA instance can protect [7], or

(iii) Misappropriate signed COA instances – responsibility of the organization that issues COA instances.

From that perspective, COA can be used to protect objects whose value roughly does not exceed the cost of forging a single COA instance including the accumulated development of a successful adversarial manufacturing process (ii).

3.1 Capturing the Random Fiber Structure

There are several ways how the high dimensional structure of a fiber-based COA can be captured. The capturing process should be such that its implementation is inexpensive and that the recorded structure is hard to replicate using an inexpensive manufacturing process. We have chosen experimentally a particular design that strikes a balance between hardware cost and complexity and anti-counterfeiting resistance. We call this type of device the Sweep-line Scanner.

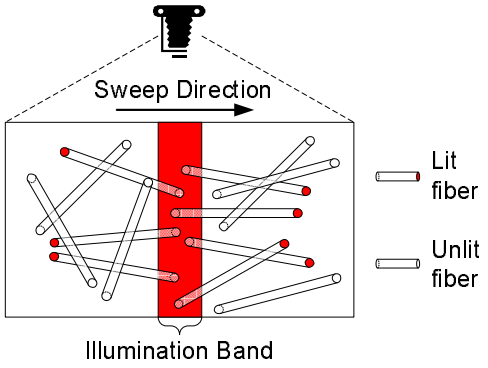

Fig. 2. The basic idea of a sweep-line fiber scanner.

The basic operating principle of a sweep-line fiber scanner is illustrated in Figure 2. A narrow beam of intense light (the *illumination band*) is swept across the COA surface in one direction. A fiber is lit when one of its two ends lies in the illumination band. If both ends of a fiber lie completely within the illumination band, it would be difficult to detect either end. This stems from the fact that the light coming out of either end, would be too weak compared with the intensity of the illumination band. Two point sets can be obtained from a sweep-line scanner: the *Left Set* (S_l) and the *Right Set* (S_r).

Definition 1. A **Left Set** S_l of a fiber-COA is a set of left-most ends of fibers as seen by our sweep-line scanner; a **Right Set** S_r that of the right-most ends.

COA's acceptance threshold is related to two matching ratios: that obtained from comparing two scans of *the same* fiber pattern (R_s) and that obtained from comparing two scans of two *different*, randomly-chosen fiber patterns (R_d). Our experiments on scores of COA instances showed that R_s is typically in the neighborhood of 85%-95%, while R_d is in the neighborhood of 10%-15%. Some of the measured errors are due to distortion caused by the camera lens. Under the assumption that this type of distortion is minimized or corrected, we expect the divergence between these two values to further increase. An acceptance threshold of 50% is sufficient for determining the authenticity of a COA with cryptographically negligible false-negative and false-positive probabilities [7].

4. CHALLENGES

We identify two crucial features encountered in the design of fiber-based COA systems: identifying fiber locations and point-set compression.

4.1 Identifying Fibers' Locations

Using the two sets of points from Definition 1, under the assumption that fibers are of relatively constant length, the reader presented in Figure 2, can identify the positions of all fibers with high likelihood of success. This procedure during detection is important as it forces the adversary to replicate the positioning of each individual fiber in the COA. In this positioning paper, as opposed to presenting an algorithm for this task, we try to formally analyze the impact of locating fibers on the economic effectiveness of the deployed COA system. We briefly compare the simplified[2] performance of two systems, the one presented in [7] and the one proposed in this paper with respect to counterfeiting cost. The system proposed in [7] forces the adversary to place only one fiber tip at an exact location on the COA field, whereas she can rest the other tip in a large area with a low likelihood of error. Obviously, the first objective is significantly more difficult but still has a relatively high probability of success p_1. In the system proposed in this paper, the adversary places the first fiber end-point with a success rate of p_1, i.e., this event is equivalent to the counterfeiting effort in the first system. However, we assume that as the other end-point must be placed at an exact location as well, the adversary in this case has a success rate of $p_2 = p_1 - \epsilon$, where ϵ is an offset that models the additional difficulty for the adversary of placing one fiber end-point while the other tip is fixed. We assume that ϵ is relatively small compared to $\epsilon \ll p_1$.

We assume that using a limited amount of storage, a reference compression scheme stores $2G$ illuminated fiber end-points into COA's barcode. In the previous system, while forging a COA instance, the adversary positions sequentially fiber end-points until $2G$ of them are at exact locations. Let's assume that the adversary has $2G$ trials to perform this task. If unsuccessful, she must try to create a new instance from scratch. The adversary uses a manufacturing mechanism which places fibers at a given position with likelihood p_1, where the placement error, $\nu = 1 - p_1$, is relatively small. We denote as $p(2G)$, the probability that the adversary has finished its job after $2G$ successful trials. Thus, the expected number of trials to forge a COA instance equals: $\chi = 2Gp^{-1}(2G) = 2Gp_1^{-2G}$. The expected number of fiber placements in case of a discarded COA instance can be computed as: $\chi_0 = (1-\chi^{-1})^{-1} \sum_{i=1}^{2G} i(1-p_1)^{i-1}p_1$. The cost of positioning a single fiber end-point during forgery is ς_e. Hence, the expected cost of forging a COA instance totals: $\varsigma_f/\varsigma_e = f(G, \chi, \chi_0) = 2G + \sum_{i=1}^{\infty}(1-\chi^{-1})^i\chi_0$. For the system proposed in this paper, we have $\chi' = 2Gp^{-1}(2G) = 2Gp_1^{-2G}\epsilon^{-G}$, then $\chi'_0 = (1-\chi^{-1})^{-1}\sum_{i=1}^{G}[(2i-1)(1-p_1)^{2i-2}p_1 + 2i(1-p_1+\epsilon)^{2i-1}(p_1-\epsilon)]$, from where we can compute the improvement in the forging cost: $\varsigma'_f/\varsigma'_f = f(G, \chi', \chi'_0)/f(G, \chi, \chi_0) \propto \mathcal{O}(\epsilon^{-G})$ if $\chi > 1$. Thus, if the adversary has <u>not</u> fully mastered the process of forging COA instances, i.e., she is expected to discard at least one instance before she successfully forges one, the improvement in the forging cost can be substantial even for small ϵ.

[2]We ignore the demand for tolerance to a small number of scanning errors.

4.1.1 *Adversarial Counterfeiting Machinery.* Counterfeiting COA instances using a device that places both ends of a fiber at a certain location as dictated by the two encoded point-sets, can be made an arbitrarily expensive routine. The cost of such a machine is dependent upon several parameters: (*i*) the thickness of fibers, (*ii*) the density of fiber end-points on the COA substrate, and (*iii*) the resolution of the scanning device. In order to balance the forging and manufacturing expenses, the COA issuer must find an optimal spot within this design space which achieves fewest manufacturing and scanning costs, while forcing the adversary into high forging expenses. For example, by assuming a COA width of 10mm and a reader based upon a 1024x768 pixel CCD sensing matrix, the manufacture already puts the precision requirement at roughly 10μm. As micron-thick fibers are inexpensive and aforementioned cameras sell under $100 nowadays, COA manufacturers can have quite an upside in the forging cost even with inexpensive COA instances. We acknowledge that as technology improves, it is likely that the counterfeiting battle is held at the forefront of nanotechnology.

4.2 Point-Set Compression

Recently, Kirovski concluded in [7] that under the constraints of: (a) fixed system storage, (b) an expectation that during manufacture, the counterfeiter is likely to throw away at least one instance per forgery, and (c) a manufacturing process in which the adversary cannot delete her placement errors, the improvement in the compression ratio for the point-set compression algorithm used in the system results in *exponential* increase in the forging cost. In this positioning paper, we evaluate only the lower bound on compressing the desired point-sets from Definition 1.

Our goal is to provide a binary representation for a set P of M distinct points $p_1, p_2, \cdots, p_M$ (that correspond to fiber end locations) with minimum number of bits possible. In the representation, the order of these points is not important. Each point is a member of a high dimensional finite integer grid $U = \{1, 2, \ldots L\}^N$. Furthermore, we assume that $\mathcal{P}$ is a uniformly-randomly-chosen within U. Let R be the total number of bits spent for compression. We observe the standard information-theoretic entropy bound that holds for any compression algorithm:

$$R \geq \log_2 \left(\begin{array}{c} L^N \\ M \end{array} \right), \tag{1}$$

where the right hand side is the *entropy* of the underlying distribution. The bound holds in expectation (i.e., on average) and one may observe individual realizations of a compression algorithm that results in smaller bit rates than the entropy.

5. APPLICATIONS

A COA of high counterfeit resistance and low manufacturing and validation cost enables a myriad of applications. The value that a COA represents should approximately equal the cost to forge (e.g.,copy, modify associated information) a copy [7]. The inexpensive verification process makes COAs particularly attractive for several traditional applications as well as for a myriad of new ones.

Checks, money orders can be signed both manually as well as with an account holder's COA scanner capable of printing barcodes. Banks, account holders, and check recipients can all verify that a certain check has been issued by a certain

bank. The framework can enable all features required to transfer, share, merge, expire, or vouch checks.

Coupons, tickets. Besides providing a relatively secure way of issuing and verifying coupons and tickets, the proposed framework enables all parties involved to reliably participate in complex business models such as third-party conditional discounts and coupon/ticket sharing and transfer.

Hard-to-copy documents. COAs can make personal ID cards (both paper and smart card based) hard to copy. In addition, they can protect and/or associate additional information to signed paper documents or artwork.

License tags, warranties, receipts. Current certificates of authenticity based on sophisticated printing technologies [16] suffer from relative ease of replication and/or license alteration. While the proposed framework for fiber-based COAs aims at remedying this deficiency, it also enables several other features such as proof of purchase/return, proof of repair, transferrable warranty, etc. Note that the COA must be firmly attached to the associated object as an adversary may remove, substitute, or attach valid COAs at will. Some of these problems can be rectified by devaluing COAs at point of sales or by recording transactions on the COA itself. For example, a license tag may consist of two independently identifiable COA instances, where one is removed at purchase time to signal a sold product. The same procedure can be used to signal and/or value product's "N^{th} owner." Finally, note that COAs complement RFID tags.

Tamper-evident seals. Particularly attractive to the pharmaceutical and postal industry, COAs, if wrapped around a product package, can verifiably seal its contents. Even a minor tear of the wrapper should cause perturbation in the random structure of the COA instance sufficient for a failed authenticity test.

6. CONCLUSION

In this paper, we proposed a novel system for automated verification of fiber-based COAs. We outlined the key challenges in enabling high cost-efficiency of such a system: identifying fibers's locations and point-set compression. The key features of the new COA scanner are simplicity, reliability, lack of any moving components, and the ability to accurately identify exact positions of individual fibers infused in COA's containing paper. The latter feature significantly increases the forging cost compared to trivial scanner implementations. Finally, we support our presentation with images of the developed scanner prototype presented in Figure 3.

REFERENCES

K. Barry. Counterfeits and Counterfeiters: The Ancient World. Available on-line at: `http://www.ancient-times.com/newsletters/n13/n13.html`

ANSI X9.62-1998. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998. On-line at: `http://www.x9.org`.

D.W. Bauder. Personal Communication.

D.W. Bauder. An Anti-Counterfeiting Concept for Currency Systems. Research report PTK-11990. Sandia National Labs. Albuquerque, NM, 1983.

S. Church and D. Littman. Machine reading of Visual Counterfeit Deterrent Features and Summary of US Research, 1980-90. *Four Nation Group on Advanced Counterfeit Deterrence*, Canada, 1991.

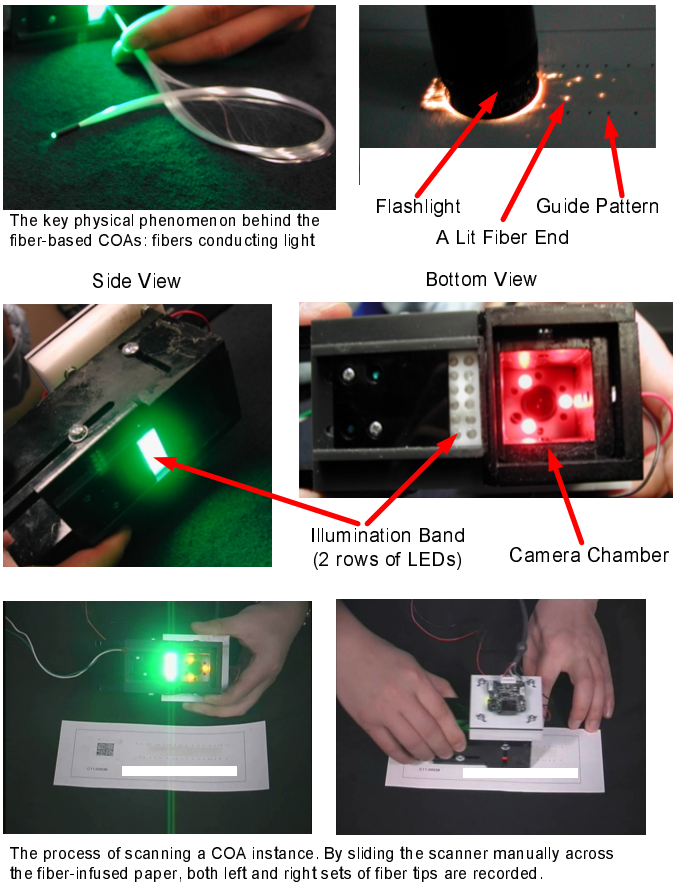

Fig. 3. The prototype of the proposed COA scanner.

IEEE 1363-2000: Standard Specifications For Public Key Cryptography, 2000. On-line at: `http://grouper.ieee.org/groups/1363`.

D. Kirovski. Toward An Automated Verification of Certificates of Authenticity. *ACM Electronic Commerce*, pp.160–9, 2004.

A.J. Menezes, et al. Handbook of Applied Cryptography. CRC Press, 1996.

Commission on Engineering and Technical Systems (CETS). Counterfeit Deterrent Features for the Next-Generation Currency Design. The National Academic Press, 1993.

R. Pappu. Physical One-Way Functions. Ph.D. Thesis, MIT, 2001.

J. Collins. RFID Fibers for Secure Applications. RFID Journal, 2004. Available on-line at: `http://www.rfidjournal.com/article/articleview/845/1/14`.

CrossID, Inc. Firewall Protection for Paper Documents. Available on-line at: `http://www.rfidjournal.com/article/articleview/790/1/44`.

Inkode, Inc. Available on-line at: `http://www.inkode.com`.

Creo, Inc. Available on-line at: `http://www.creo.com`.

RF SAW, Inc. Available on-line at: `http://www.rfsaw.com/tech.html`

R.L. Van Renesse. Optical Document Security. Artech House, 1998.

R. L. Rivest, et al. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol.21, no.2, pp.120–126, 1978.