

# FiberFingerprint Identification

## Eric Métois

Escher Labs  
Escher Group Ltd.  
Cambridge, MA - USA  
metois@eschergroup.com

## Paul Yarin

Escher Labs  
Escher Group Ltd.  
Cambridge, MA - USA  
yarin@eschergroup.com

## Noah Salzman

Escher Labs  
Escher Group Ltd.  
Cambridge, MA - USA  
noah@eschergroup.com

## Joshua R. Smith

Escher Labs  
Escher Group Ltd.  
Cambridge, MA - USA  
jrs@eschergroup.com

## Abstract

*We present an identification system based on the naturally occurring inhomogeneities of the surface of paper. We investigate the scaling of its performance for verification and identification through a general and rigorous framework and present a random coding argument that links biometric identification to communication through a noisy channel. We measure the effective communication rate and information density for various configurations of the system.*

## INTRODUCTION

The possibility of authenticating products or documents by matching difficult-to-duplicate, inhomogeneous or “random” structure to an associated description of the genuine article has been investigated in various contexts [1] [2]. Escher Labs’ FiberFingerprint technology uses the naturally occurring irregularities of a substrate as a means to discriminate between various documents or objects.



Figure 1. FiberFingerprint verifier for mail piece

The practical motivation for this technology is security. Compared to a barcode, digital watermark, or other embedded serial number, the identity of a FiberFingerprinted object is difficult to forge, given the length scale and three-dimensional aspects of the physical properties being sampled. This paper considers the use of such random inhomogeneities for item identification, rather than simple authentication. A database of samples of the random characteristic is maintained. When an item to be identified is submitted, its random characteristic is measured and compared to the database to find the best match.

We investigate the scaling of the performance of such an identification system. In [3], one of us performed a related study using randomly assigned, noiseless IDs. In the present context, we again are using randomly assigned identifiers, but have dropped the assumption of noiselessness: each time a particular object is sensed, somewhat different data is collected because of noise.

## Verification versus identification

From a general point of view, the system’s main function is to compare fingerprints and to assess the degree to which they match.

In the context of the verification problem, the system will typically be provided with an observation of an object, and a claimed identity for that object. The task of the system is to compare two fingerprints. The first is recalled from a database, based on the claimed identity, and the second is extracted from the observation of the presented object. The system is expected to assess whether a particular match is “good enough”.

In the context of the identification problem, the task of system is to infer the identity of the object based on its fingerprint. Without any particular claim concerning the object’s identity, it is natural to assume that the object’s fingerprint has to be matched against a possibly large number of fingerprints that may be stored in a database in order to assess “the best match”.

Hence, while the two systems may use the same numerical criterion to evaluate the match between fingerprints (e.g. error rate, distance, correlation, etc.), their ultimate decision rules will differ. Salient performance characteristics should reflect these differences.

## Motivations and overview

In a careful attempt to quantify the performance of our FiberFingerprint approach, we have investigated means to measure salient performance characteristics. Along with the actual performance data, these means are the main object of this document. Because of our approach’s obvious similarities with biometrics and auto-identification, we believe that this performance analysis may be relevant outside the specific context of our FiberFingerprints.

In what follows, we will first describe the fundamentals of the FiberFingerprint technology. We will present salient performance characteristics in the context of verification and identification. We will describe our testing environment and propose a means to extrapolate the performance statistics we seek from our observations. Lastly, we will present an analogy between identification systems and communication systems that provides a simple framework for understanding our performance results.

## FIBERFINGERPRINT TECHNOLOGY

### System overview

The system uses registration marks to identify the area of the medium that should be analyzed. These registration marks typically consist of a few small dots, spanning a total surface area of typically less than 25 mm<sup>2</sup>. The imager consists of a consumer-grade video module and lens, housed along with the appropriate lighting apparatus. The imager provides a grayscale capture of the medium's texture to the software responsible for the FiberFingerprint analysis.



Figure 2. Imager and objects (tokens) used for this study

The FiberFingerprints reported on here are derived from a one-dimensional signal, the Fiber Signal, which is extracted from the two-dimensional capture along a series of linear segments. These linear segments constitute the Signal Path, and they are an important part of the system's configuration. The detection of the registration mark provides all the relevant translation, rotation and scaling information that is needed in order to overlay the Signal Path with the captured image of the substrate texture.

Running along the Signal Path, a raw signal is extracted by averaging pixel values along the transverse direction of the signal path. The spatial sampling frequency that is used at this stage is also a part of the system's configuration.

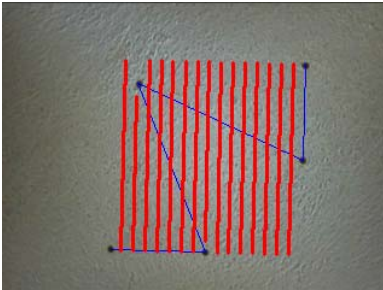


Figure 3. Sample capture from the imager; overlaid lines connecting the registration dots (blue) and Signal Path (red)

The resulting one-dimensional raw signal is subsequently high-passed. From the perspective of the original image, this is a high-pass filtering stage in the longitudinal direction of the Signal Path. The resulting filtered signal is finally re-sampled and normalized in order to lead to the Fiber Signal. The FiberFingerprint is a quantized and optionally formatted version of the Fiber Signal.

### Matching criterion

As a means to score the match between two *Fiber Signals* and in the absence of any prior information concerning the probability distributions of the data, computing correlation coefficients naturally comes to mind. As we further wanted to express this criterion in terms of an error rate, we chose the following measure.

$$\varepsilon(X, Y) = \frac{1}{2} \left[ 1 - \frac{X^T Y}{\|X\| \|Y\|} \right], \text{ where } X \text{ and } Y \text{ are two } Fi-$$

*ber Signals* (as vectors of length N).

Whether we are considering the verification problem (i.e. comparing this error measure to a fixed threshold), or the identification problem (i.e. searching for a minimal value of this error measure), the conditional probability distributions  $\varepsilon_G$  of our matching criterion under the Genuine (i.e. X and Y identify the same object) and the conditional probability distributions  $\varepsilon_C$  of our matching criterion under the Counterfeit (i.e. X and Y identify different objects) hypotheses are key to the performance evaluation of our system.

### Chosen configurations

In the context of the present work, we've chosen to consider a range of different configurations for our FiberFingerprint analysis. All configurations share the same registration marks (illustrated above in Figure 3). All configurations can therefore be tested on the same test data. For all configurations, the FiberFingerprint is an 8-bit quantized version of the Fiber Signal but the length of the Fiber Signals is different among the configurations, ranging from 50 to 300 samples.

## RELEVANT STATISTICS

### Performance of a verification system

We wish to determine whether two provided fingerprints X and Y identify the same object or not. In order to do this, we compute the error rate that relates the two provided fingerprints and compare the result to a fixed threshold.

### Probabilities of false positives and false negatives

The performance of such decision rule is typically evaluated in terms of the probabilities of false positives and false negative matches.

A false positive will occur when a genuine match was found between two fingerprints that identify two different objects. The probability for this type of false to happen (FP) is a direct function of the distribution of the error rate under the counterfeit hypothesis and the value of the fixed threshold.

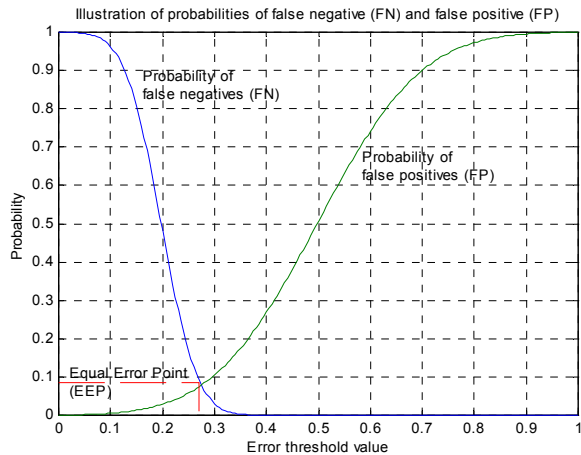
$$FP(\alpha) = \Pr\{\varepsilon_C < \alpha\} = \int_0^\alpha p_{\varepsilon_C}(u) du$$

A false negative will occur when two fingerprints identifying the same object don't match with a sufficient accuracy. The probability for this type of false to happen (FN) is similarly derived.

$$FN(\alpha) = \Pr\{\varepsilon_G > \alpha\} = 1 - \int_0^\alpha p_{\varepsilon_G}(u) du$$

### Equal error point

As visualizations of the verification system's performance, it is common to see plots of these two functions on the same graph, as functions of the threshold value.



**Figure 4. Typical false positive and false negative curves**

The performance of the system is obviously related to the amount of overlap between FP and FN. The *Equal Error Point* (EEP) corresponds to the regime where the threshold value was chosen such that FN and FP are equal. While verification systems are rarely tuned to operate at this regime, the *Equal Error Point* is often used as a convenient measure of a system's performance.

### Receiver operating characteristic

It is also common practice to plot one type of false as a function of the other. For instance, a *Receiver Operating Characteristic* plot (ROC) will graph the probability of true positives (1-FN) versus the probability of false positives (FP). The area beneath the resulting ROC graph is known as the *Figure of Merit*. Its value is bounded above by 1 (perfect performance) and below by 1/2 (random decision rule).

### Performance of an identification system

An identification system will most likely be provided with a single fingerprint and the task to find the "best match" among a pre-recorded database of objects. Hence, the system will not base its decision on the relationship between a single measure of the error rate criteria and a fixed threshold. Rather, it will implement the following decision rule:

$$ID = \arg \min_{k \text{ s.t. } Y_k \in \Omega} \varepsilon(X, Y_k),$$

where  $k$  stands for an index of known objects for which fingerprints  $Y_k$  were recorded in a database  $\Omega$ .

### Probability of false identification

Errors resulting from such a decision rule have a different nature and probability than the false positives and the false negatives we discussed previously.

Suppose that the system is presented with a fingerprint  $X$  of an object that is known the database  $\Omega$ . Let  $k_0$  be the index associated with that object and let  $M$  be the number of objects in the database. The *Probability of False Identification* (FID) can be expressed as follows.

$$\begin{aligned} FID_M &= \Pr\{\exists k \neq k_0 \text{ s.t. } \varepsilon(X, Y_k) < \varepsilon(X, Y_{k_0})\} \\ &= 1 - \Pr\{\forall k \neq k_0, \varepsilon(X, Y_k) > \varepsilon(X, Y_{k_0})\} \end{aligned}$$

Further assuming that successive matching attempts are independent events, we can relate the *Probability of False Identification* for various database sizes  $M$ . More specifically, we can relate it to the elementary case where there are only two known objects in the database (i.e. the correct answer and a wrong answer):

$$FID_M \approx 1 - (1 - FID_2)^{M-1} \quad (\text{eq. 1})$$

Recalling the conventions we've introduced earlier for the conditional distributions of the error rate in the Genuine and the Counterfeit hypotheses, the *Probability of False Identification* in the elementary case of  $M=2$  can be expressed as follows:

$$FID_2 = \Pr\{\varepsilon_G > \varepsilon_C\} = \int_0^\infty p_{(\varepsilon_G - \varepsilon_C)}(u) du \quad (\text{eq. 2})$$

### Probability of collisions in a fingerprint database

In the previous derivation of the *Probability of False Identification*  $FID_M$ , we've simply assumed that we already had a valid database of  $M$  objects. In practice, the  $M$  objects will most likely be enrolled on an as-needed basis and we'll hope that the resulting set is free from collision. In other words, we'd like to make sure that as a new object gets enrolled, its fingerprint is sufficiently different from those of the objects that were enrolled up until this point. This problem is related to the classic "birthday problem".

Let  $PNC_M$  be the probability that a randomly chosen set of  $M$  fingerprinted objects constitutes a database with no collision. Let  $e_k$  denote the event that at the stage when the  $k^{\text{th}}$  object is enrolled, it is not falsely identified as any of the  $(k-1)$  objects that were previously enrolled. Using the chain rule for probabilities, we can express  $PNC_M$  as follows.

$$PNC_M = \Pr(e_2) \Pr(e_3 | e_2) \dots \Pr(e_M | e_{M-1}, \dots, e_2)$$

Recalling our definition for the *Probability of False Identification*  $FID_M$  and (eq. 1),

$$\Pr(e_k | e_{k-1}, \dots, e_2) = 1 - FID_k \approx (1 - FID_2)^{k-1}$$

$$\text{and therefore: } PNC_M \approx (1 - FID_2)^{M(M-1)/2}$$

### Number of identifiable objects

The previous formula relates the probability that M randomly chosen objects may be reliably identified from their fingerprints to  $FID_2$ , the *Probability of False Identification* in the elementary case of  $M=2$ . It clearly illustrates the fact that for a reasonable number of objects (i.e. over 100), the false match rate  $FID_2$  must be small.

If  $FID_2$  is indeed small and M is large enough, then M can be approximated by this expression:

$$M \approx \sqrt{\frac{-2 \ln(PNC_M)}{FID_2}} \quad (\text{eq. 3})$$

The number of randomly chosen objects that can be reliably identified through their fingerprints is the ultimate performance measure of the system in the context of the identification problem. In what precedes, we've shown how to relate this number to an elementary probability of false identification, which can be derived from the error rate distributions.

### Cumulative match score

As a means to evaluate the performance of an identification system, it is noteworthy that some studies (such as [7]) use the concept of a *Cumulative Match Score* (CMS). Provided with a number M of objects, the CMS is the proportion of the identification attempts for which the best match is the correct answer. Using our convention, it is the complement of the *Probability of False Identification*.

$$CMS_M = 1 - FID_M \approx (1 - FID_2)^{M-1} \quad (\text{eq. 4})$$

## OBSERVED ERROR RATE DISTRIBUTIONS

We now wish to estimate the statistics we've previously identified in the context of our actual FiberFingerprints. In order to do so, we shall collect a set of images, extract FiberFingerprints, and measure error rates for genuine cases (comparing fingerprints of the same objects) and counterfeit cases (comparing fingerprints different objects).

### Data set

Consumer-grade self adhesive paper stock was affixed to 30 small plastic tokens and a registration mark (a constellation of five dots) was printed on each one. Using our FiberFingerprint imager, we captured 25 snapshots of each of the 30 tokens, leading to a total of 750 images (320x240 pixels each). The genuine trials correspond to FiberFingerprint error rates that are measured when images are matched against different captures of the same object. The total number of genuine trials is  $750 \times 24 = 18,000$ . There are a potentially large number of counterfeit matches but as a means to balance our observations, we chose to retain a subset: each one of the 750 images is matched against a

single capture of the 29 other objects. This leads to a total of  $750 \times 29 = 21,750$  counterfeit trials.

### Observed error rates

A histogram of the observed error rates provides an estimate of the probability distributions of the error rate under the genuine and the counterfeit hypotheses.

Using 200-byte FiberFingerprints, it is worthwhile to note that out of the 39,750 observations of error rates, the maximum value for the error rate we observed among the genuine trials was 0.3130, while the minimum value for the error rate we observed among the counterfeit trials was 0.3658.

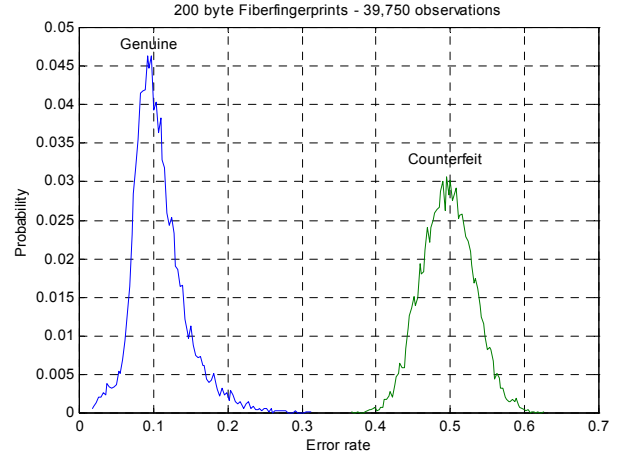


Figure 5. Observed error rate distributions; histograms

In other words, no overlap between these two histograms was observed. This is mixed news in the sense that on one hand, it hints to a high performance of our FiberFingerprinting system, but on the other hand, we are unable to read an estimate of the performance evaluation statistics discussed earlier.

## EXTRAPOLATION FROM THE OBSERVED ERROR RATE DISTRIBUTIONS

### Motivation and proposal

The statistical performance characteristics we seek are beyond the scope of what we could observe over our test trials. We propose to extrapolate our observation by fitting well-behaved curves to the histograms of our observations in order to obtain estimates for these characteristics. The purpose of our fit is to extrapolate statistics in the overlap region of the genuine and the counterfeit distributions, not to summarize the statistics that were obtained from the distribution. Therefore, the fit should prioritize the area of interest, to the detriment of the overall fit if necessary.

In the genuine case, the error distribution (derived from correlation coefficients) will systematically have a noticeable asymmetry. We propose nevertheless to extrapolate both genuine and counterfeit cases with Gaussian distributions, insisting once again that the fit is specifically limited to the overlap region.



### Fit to the observed data

The error distribution curve in the counterfeit case is fit with a Gaussian distribution, the mean and variance of which are set to the observed sample mean ( $\hat{m}_C$ ) and the unbiased estimate of the observed variance ( $\hat{\sigma}_C^2$ ).

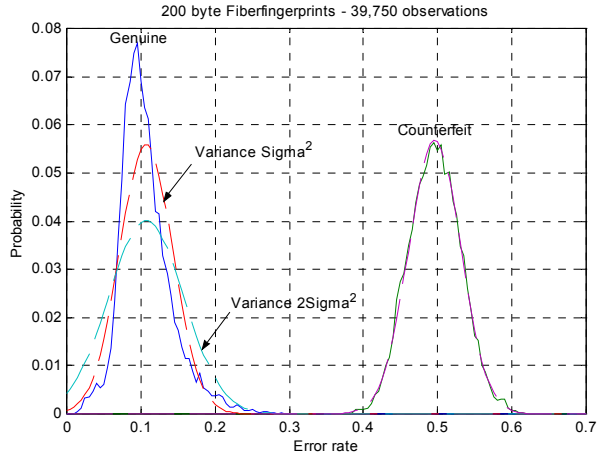


Figure 6. Fitting Normal distributions to the observations

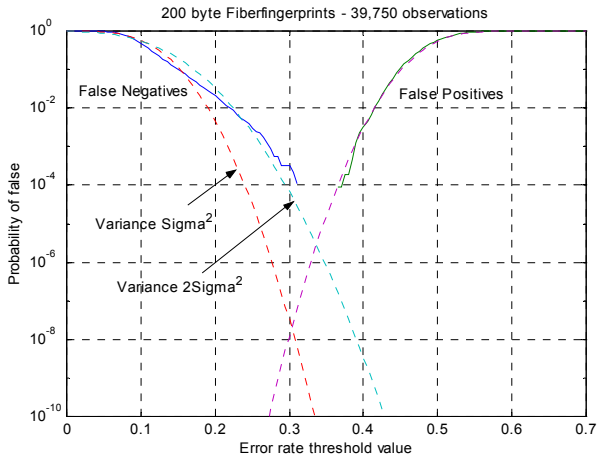


Figure 7. Extrapolation of the cumulative functions

For the genuine case, we found that doubling the observed variance ( $2\hat{\sigma}_G^2$ ) while using the sample mean ( $\hat{m}_G$ ) lead to a fairly accurate fit near the overlap region. As we suggested earlier, this extrapolation of the tail region of interest is done to the detriment of the overall fit.

### RELEVANT STATISTICS FROM THE EXTRAPOLATED DISTRIBUTIONS

#### Performance as a verification system

We recall that the *Equal Error Point* (EEP) is a convenient measure of a system's performance in the context of the verification problem. It corresponds to the probability of false in the regime where the decision threshold was set to:

$$\alpha_0 \text{ such that } FN(\alpha_0) = FP(\alpha_0) = EEP$$

The error rate observations we collected were unable to provide us with an estimate for this value from the histograms. The extrapolation discussed above provides a means to extend these histograms in their overlapping region, and derive an extrapolated value for the EEP.

In fact, the choice of Gaussian distributions for the extrapolation allows us to derive a closed form for the estimated *Equal Error Point* as a function of the sample means and variances of the observed error rates.

$$EEP = \frac{1}{2} \left[ 1 - \text{Erf} \left( \frac{\hat{m}_C - \hat{m}_G}{\sqrt{4\hat{\sigma}_G^2 + \sqrt{2\hat{\sigma}_C^2}}} \right) \right]$$

The following illustrates numerical values that are obtained for this estimate in the context of our configurations.

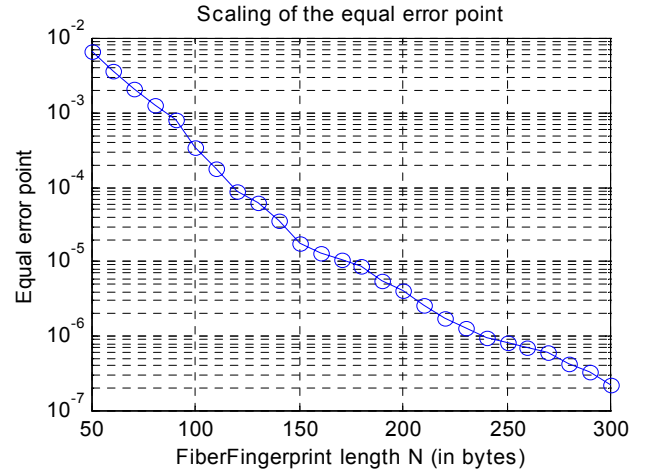


Figure 8. Extrapolated estimates of the Equal Error Point

As a means to provide some sense of scale, such values for the EEP are very good by any biometric standards. Indeed, a good fingerprint matching algorithm will typically yield to an EEP in the  $[10^{-3}, 10^{-2}]$  range [8]; voice recognition systems have a typical EEP in the  $[10^{-2}, 10^{-1}]$  range [9]; and iris scan systems top all other biometric systems with an EEP in the  $10^{-6}$  range [9].

#### Performance as an identification system

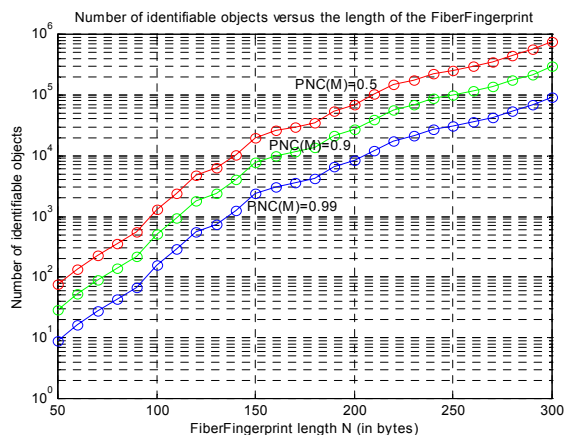
We recall that in the context of the identification problem, our ultimate performance evaluation characteristic is the estimate of the number of randomly chosen objects that may be identified reliably from their FiberFingerprints. We've previously defined the *Probability of False Identification* for a database of  $M$  known objects ( $FID_M$ ) and showed (eq. 1) that it can be easily derived for any  $M$  from the elementary case where  $M=2$ . We've further related  $FID_2$  to our ultimate number of identifiable objects (eq. 3). Hence  $FID_2$  is a crucial performance characteristic.

The lack of observed data in the overlapping region of the error rate distributions prevented us from reading this probability of false identification from the histograms. As for the verification case, the Gaussian extrapolation we've proposed provides a means to extend these histograms in

their overlapping region, and derive an extrapolated value for the  $FID_2$ . Once again, the choice of Gaussian distribution allows us to derive a closed form for the characteristic we seek from (eq. 2).

$$\hat{FID}_2 = \frac{1}{2} \left[ 1 + \text{Erf} \left( \frac{\hat{m}_G - \hat{m}_C}{\sqrt{4\hat{\sigma}_G^2 + 2\hat{\sigma}_C^2}} \right) \right]$$

Recalling (eq. 3), we can further estimate the number of identifiable objects  $M$  from our observations and chosen values for  $PNC_M$ . Again,  $PNC_M$  is a measure of the certainty with which a randomly chosen set of  $M$  objects will constitute a valid FiberFingerprint database. In practice, we will typically fix its value to a level we feel comfortable with, and figure out the associated value for  $M$  with this degree of comfort. Figure 9 illustrates the numerical values we obtained for this estimate in the context of our chosen configurations, and 3 fixed values for the probability of no collision (0.5, 0.9 and 0.99).



**Figure 9. Extrapolated number of identifiable objects**

These estimates suggest that, using our most conservative reliability standard ( $PNC = .99$ ), around ten thousand objects should be reliably identifiable using FiberFingerprints consisting of 200 x 8-bit values, and around 100,000 items should be reliably identifiable using 300 x 8 bit FiberFingerprints using our implemented system.

Once again in order to provide a sense of scale, a recent study of various face recognition algorithms [7] suggests that the best systems yield to *Cumulative Match Score* in the neighborhood of  $CMS = 0.97$  for a database of 1200 faces. Recalling our prior discussion of  $CMS$  (eq. 4), this translates into  $FID_2 = 2.5 \cdot 10^{-5}$ . Plugging this value in (eq. 3) implies that such system could only identify about 100 faces reliably according to our criteria.

By imaging larger texture regions, we could generate larger FiberFingerprints. For example, by imaging twice the area we could generate 600-sample FiberFingerprints. We saw that increasing the number of samples from 200 to 300 increased the number of identifiable objects by roughly a factor of 10. If the identification performance continues to

scale at this rate, then adding 300 samples multiplies the number of identifiable objects by a factor of 1000. So if, with some fixed reliability, we can identify 50,000 objects using 300 samples, then we should be able to identify 50 million objects using 600 samples and 50 billion objects using 900 samples.

## IDENTIFICATION PERFORMANCE AND COMMUNICATION RATE

The problem of identifying  $M$  objects can be mapped onto the problem of communicating one of  $M$  messages (that is,  $d = \log_2(M)$  bits) through a channel. Indeed, we can view the FiberFingerprints ( $N$  bytes long each) as randomly chosen code words, which our system uses to convey one of  $M$  different messages (i.e. the identity of the object). This is essentially a communication system equivalent to our identification problem. The binary representation of the token identifier is a source message (binary just because we wish to use bits as our information measure). The FiberFingerprint collected for a particular piece of paper at enrollment time is a code word. The FiberFingerprint collected later, at identification time, corresponds to a received codeword, corrupted by channel noise. The table that maps token identifiers (messages) to FiberFingerprints (code words) is a random code, with rate  $d/N$ .<sup>1</sup> Random codes have been studied extensively in the information theory literature. They are known to exhibit good performance for large block sizes. They are not used for practical communication systems because of their large memory requirements (proportional to the number of possible messages). However, for the identification problem, we need one database entry per possible message in any case, so the memory requirement is unproblematic.

The key insight provided by the communication picture is that the number of effective bits of identification should scale linearly with the length of the FiberFingerprint. Put another way, the number of objects that can be identified grows exponentially with the length of the FiberFingerprint.

### Relationship with the identification system's performance

Viewing the system from a communications perspective, we are effectively transmitting  $d = \log_2(M)$  bits worth of information with  $N$ -byte long code words. As illustrated in Figure 10, we find overall the expected near-linear relationship between source bits and channel symbols. The three curves corresponding to different values of  $PNC$  can be viewed as different parameter settings used in the design of the random code.

<sup>1</sup> This is complicated somewhat by the fact that the FiberFingerprints actually consist of  $N$  amplitude values with 8 bits of dynamic range.

The communication rate,  $R$ , for each configuration of the code can be calculated in bits per sample by dividing the number of bits communicated,  $d$ , by  $N$ . Figure 11 shows a plot of  $R$  vs  $N$ .

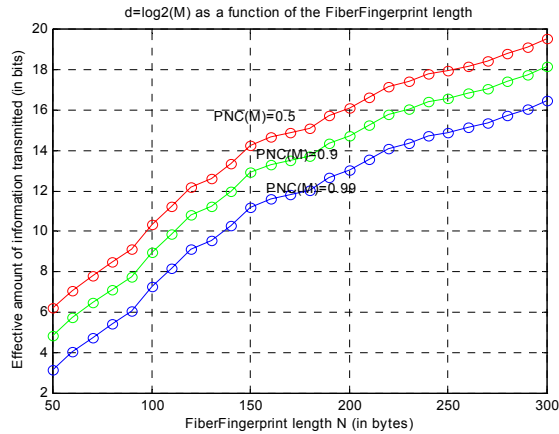


Figure 10. Effective amount of information transmitted

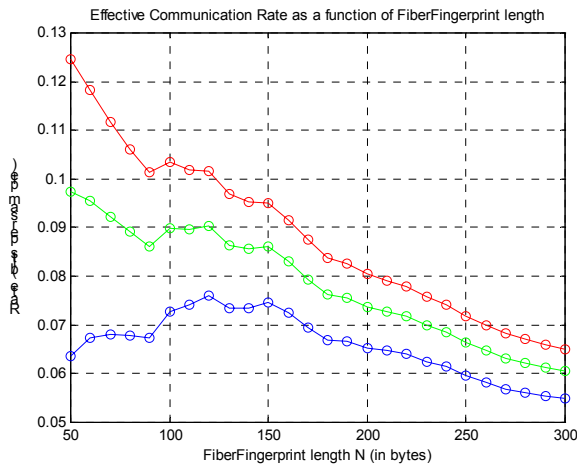


Figure 11. Effective communication rate.

Practical coding schemes are characterized by plotting the achieved bit-error-rate (per-bit probability of error) as a

function of  $\frac{E_b}{N_0} \equiv \frac{SNR}{R}$ , where SNR is the signal to noise

ratio. The various configurations of our system could be evaluated in this fashion and compared with one another, to other communication schemes, and to theoretical performance limits.

### Information Density

An important parameter of paper-based communications systems, such as barcodes, is information density. Consulting figure 10 we see that 300-sample FiberFingerprints yield around 16 bits of identification (at  $PNC = .99$ ). If we required an area of  $25 \text{ mm}^2$  for the set of 300 samples, then the effective information density of the system would be  $.64 \text{ bits / mm}^2$ . Put another way, each effective identification bit would “occupy” or require around  $1.6 \text{ mm}^2$  of physical area for this particular configuration.

## CONCLUSION

We have presented a practical, low cost, identification system based on paper texture. It has numerous potential applications in document and product security. We have presented evidence that we can reliably identify  $10^4 \sim 10^5$  randomly selected items, and it appears, based on the scaling studies, that we should be able to identify on the order of  $10^6$  items with our present system with no further change to the system’s hardware. By increasing the amount of substrate imaged, it should be possible to scale up the number of identifiable items as much as desired.

Based on difficult-to-duplicate physical structures of an object, FiberFingerprinting exhibits a degree of security that is similar to biometric systems. In contrast, printing machine-readable data, encrypted or not, does not provide the same copy protection. A further practical benefit of FiberFingerprint Identification over printed symbologies such as barcodes is that no variable printing is required. Suitable registration marks can be added to the object using various means and with commercial off-the-shelf scanning technology, it should be possible to read FiberFingerprints at manufacturing line or printing press speeds.

This paper has also suggested a parallel between random coding and biometric identification that guided our scaling investigations and could prove useful in the context of other biometric systems.

Many of the benefits of random ID assignment outlined in [3] also apply to the systems discussed here: the burden of centrally managing the ID assignment process may be reduced.

Even with the limited amount of physical area we have sampled on the tokens described in this study ( $25 \text{ mm}^2$ ), we have found verification and identification performances that surpass most commonly used biometric systems such as human fingerprints. The fact that registration issues are greatly simplified, as compared to ordinary biometric systems, is a key to this system’s high performance. Also, unlike human fingerprints, iris scans, or virtually any biometric, the performance of a FiberFingerprint system will naturally scale with the amount of physical area that is examined, and there is no hard limit on that amount. Thus the performance delivered by the system can be tuned to the performance requirements by scaling the amount of sampled paper structure as desired.

All these benefits lead us to believe that for some identification applications, FiberFingerprinting offers unique advantages as a “biometric” system for physical documents and objects.

## REFERENCES

- [1] Joshua R. Smith and Andrew V. Sutherland. Microstructure Based Indicia. Proceedings of AutoID’99, 28-29 October 1999, Summit New Jersey.

- [2] Robert N. Goldman. Non-counterfeitable document system. US patent US4423415. Light Signatures, Inc., Los Angeles, CA
  - [3] Joshua R. Smith. Distributing Identity. IEEE Robotics and Automation Magazine, pps 49-56. Vol. 6, No. 1, March 1999.
  - [4] James L. Wayman. Error-Rate Equations for the General Biometric System. IEEE Robotics and Automation Magazine, pps 35-48. Vol. 6, No. 1, March 1999.
  - [5] Athanasios Papoulis. Probability, Random Variables, and Stochastic Processes. McGraw-Hill editions. 1991.
  - [6] Claude E. Shannon. A Mathematical Theory of Communication. Bell Sys. Tech. Journal, 27: 379-423, 623-656, 1948.
  - [7] Face Recognition Technology (FERET) program. <http://www.itl.nist.gov/iad/humanid/feret/>
  - [8] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain. FVC2000: Fingerprint Verification Competition. <http://bias.csr.unibo.it/fvc2000/>
  - [9] Ken Phillips for PC Week Labs. Unforgettable biometrics. 1997. Available online from [www.zdnet.com](http://www.zdnet.com)
- Note: the technologies described in this paper are patent pending. Please address correspondence to Joshua R. Smith, [jrs@eschergroup.com](mailto:jrs@eschergroup.com).