Fingerprinting Long Forgiving Messages

G. R. Blakley
*C. Meadows**
G. B. Purdy
Department of Mathematics
Texas A&M University
College Station, Texas 77843-3368

In his 1983 paper, Neal Wagner[1] defines a *perfect fingerprint* to be an identifying fingerprint added to an object in such a way that any alteration to it that makes the fingerprint unrecognizable will also make the object unusable. A perfect fingerprinting scheme for binary data would seem difficult to devise, since it would be possible to discover the fingerprints by comparing different fingerprinted copies of the same piece of data. In this paper we discuss a fingerprinting scheme which, although it does not surmount this problem entirely, at least specifies the number of copies an opponent must obtain in order to erase the fingerprints.

The fingerprints involved will be rather lengthy, so we will restrict ourselves to what we will call *long forgiving messages.* A forgiving message is one which is still readily understandable and not jarring when up to 0.1% of it has been altered. Examples are voice and television. People can speak comfortably amid the noise of a cafeteria and can enjoy watching a television show with several pixels per frame altered. The idea in each case is that the support of the noise (the set outside which the additive noise must vanish) must have small

*Now at Computer Science and Systems Branch, Naval Research Laboratory, Washington, D. C. 20375.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 180-189, 1986.

measure. We must also require that our messages not be *too* forgiving, since otherwise it would be possible to erase the fingerprints by adding random noise and still have a usable message.

Let P be a long forgiving message (for example, a digital TV show). We wish to protect P from piracy by adding a different fingerprint F to each copy of P in such a way that a pirate who wishes to copy P+F and distribute it illicitly cannot erase the information about the origin of P contained in F unless he has obtained a certain predetermined number of different copies. We will define a *d out of n fingerprint scheme* to be one in which n objects are fingerprinted, and in which the pirate must obtain d copies in order to erase the fingerprint from one copy. A fingerprint F must also obey the following constraints: If we think of the M-tuples P and F as functions from the set {1,2,...,M} to $\mathbf{Z}_2$ then

[a] Supp(F), the subset of {1,2,...,M} outside of which F vanishes, must be small enough so that F does not interfere with the viewability of the program.

[b] Supp(F) must be large enough so that F cannot be eradicated by random noise without affecting the usability of the message.

We construct the n fingerprints, F_1 through F_n in the following manner. Fix an integer k. For each subset A of {1,2,...,n} of cardinality $\leq$k, choose a subset S(A) of {1,2,...,M} such that $A \neq B \Rightarrow S(A) \cap S(B) = \phi$. Then let

$$F_i = \sum_{i \in A} \chi(S(A))$$

where χ denotes the characteristic function. Note that n must be equal to

$$\sum_{j=1}^{k} \binom{M}{j}$$

and so k must be relatively small.

Suppose that the pirate has obtained copies 1 through l, with fingerprints F_1 through F_l, and that he wants to erase the fingerprint from $P + F_1$ by adding some function E to it so that the origin of $P + F_1 + E$ is not ascertainable by the owner. (We use the word *owner* to mean the owner of the pristine copy.) Ideally, of course, he would like E to be F_1, but if not, at least he would like E to be the sum of some $\chi(S(A))$s such that $1 \in A$ and some $\chi(S(A))$s such that $1 \neg\in A$ (where $\neg$ denotes the logical not). The former will serve to cancel out various components of F_1, and the latter will serve to give the owner misleading information about the origins of the other copies that the pirate has obtained. Of course, the pirate would prefer, in order to give the most misleading information possible, to add on characteristic functions of sets S(A)) such that $A \cap X = \phi$, Since he has absolutely no way of finding out such an S(A) (except by obtaining more copies), he is reduced to adding on some random function R if he wishes to do this. However, the support of R must be relatively small in order not to interfere with the usability of the message. It follows that the probability that the intersection of Supp(R) and any S(A) will be large enough to mislead the owner is small, and therefore that the addition of a random function will not be useful in hiding information.

Thus the pirate's best options are either to add on various $\chi(S(A))$s that he knows or to add on functions whose supports are randomly chosen subsets of the S(A)s. However, he usually cannot find out the various S(A)s directly. What he *can* find are the sets at which the copies he possesses differ from each other. In particular, for each subset A of $X = \{1,2,...,l\}$ of cardinality $\#(A) \leq l/2$, he can compute the set B(A)=

$$\{x \epsilon Y \mid (P + F_i)(x) = (P + F_j)(x) <=> i, j \epsilon A \text{ or } i, j \neg \epsilon A\}.$$

(There is no point in computing B(A) for #(A) > l/2, since B(A) = B(X–A).) For example, B({1}) is the set of all points at which $P + F_1$ differs from all other of the $P + F_i$s. An element x would either be in B({1}) because $x \epsilon \text{Supp}(F_1)$ and $x \neg\epsilon \text{Supp}(F_2)$ through $\text{Supp}(F_l)$, or because $x \neg\epsilon \text{Supp}(F_1)$ but $x \epsilon \text{Supp}(F_1)$ through $\text{Supp}(F_l)$. Similarly, B({1,2}) is the set of all points at which $P + F_1$ and $P + F_2$ agree with each other but differ from the rest of the F_is, and so on. Thus, if $1 \epsilon A$, adding on $\chi(B(A))$ to $P + F_1$ is the same as changing $P + F_1$ at all points at which it agrees with the copies in A and disagrees with the copies not in A. For example, adding $\chi(B(\{1,2\}))$ to $P + F_1$ is the same as changing $P + F_1$ at all points at which it agrees with $P + F_2$ and disagrees with all the other copies the pirate possesses.

Lemma 1. *If #(A) < l - k, then*

$$B(A) = \bigcup\{S(C) \mid \#(C) \leq k \text{ and } C \cap X = A\}$$

and if #(A) ≥ l - k, then

$$B(A) = \bigcup\{S(C) \mid \#(C) \leq k \text{ and } [C \cap X = A \text{ or } C \cap X = X - A]\}$$

where $\bigcup\{X \mid Y\}$ *denotes the union of all sets X with property Y.*

Proof. Suppose $x \epsilon B(A)$. Then all the $P+F_i$s such that $i \epsilon A$ agree at x and disagree at x with all the $P+F_j$s such that $j \epsilon X–A$. Thus either

$$x \epsilon \bigcap\{\text{Supp}(F_i) \mid i \epsilon A\} = \bigcup\{S(C) \mid \#(C) \leq k \text{ and } C \cap X = A\}$$

or

$$x \epsilon \bigcap\{\text{Supp}(F_i) \mid i \epsilon X–A\}$$
$$= \bigcup\{S(C) \mid \#(C) \leq k \text{ and } C \cap X = X–A\}.$$

Conversely, if x is in either of these sets, then all the $P+F_i$s agree at x and disagree with all the $P+F_j$s such that $j \epsilon X–A$, and so $x \epsilon B(A)$.

Thus the second part of the lemma follows. However, if #(A) > l-k, then #(X–A) > k, and thus there is no C of cardinality ≤ k such that C∩X = X–A. Thus the first part of the lemma follows. **QED.**

The following corollary tells us that if the number of copies the pirate possesses is large enough, then he has enough information to erase the fingerprints entirely.

Corollary 2. *If $l > 2k$, then*

$$\bigcup\{B(A) \mid 1 \in A\} = Supp(F_1).$$

Proof. If l > 2k, then #(A) < l - k for all subsets A of X = {1,2,...,l} of cardinality ≤ l/2. It follows from Lemma 1 that

$$B(A) = \bigcup\{S(C) \mid \#(C) \leq k \text{ and } C\cap X = A\}.$$

We thus have

$$\bigcup\{B(A) \mid 1 \in A \text{ and } A\subseteq X\} =$$

$$\bigcup\{S(C) \mid 1 \in C \text{ and } \#(C) \leq k\} = Supp(F_1).$$

QED.

Thus in the case $l > 2k$, the pirate can determine F_1 and add it to $P + F_1$ in order to obtain a pristine copy P.

Suppose that $l \leq 2k$. We will show that in this case the pirate who seeks to obtain a pristine copy of P by adding on various χ(B(A)s not only cannot mislead the owner but risks giving him even more information then before.

Lemma 3. *Let $E = F_1 + Q$ where Supp(Q) is the union of some set of B(A)s. Suppose that there exists a t such that no S(A) where $\#(A) \leq t$ appears in Supp(E). If some S(A) such that $\#(A) = t + 1$ appears in Supp(E), then $A \subseteq X$.*

Proof. Suppose that A $\neg\subseteq$ X. Then #(A∩X) ≤ t and so S(A∩X) does not appear in Supp(E) by hypothesis. By Lemma 1, we have S(A)⊆B(A∩X) and S(A)∩B(C) = ϕ for any other C ⊆ X. Therefore

$B(A \cap X)$ appears in Supp(E). We thus have only two possibilities. Either $1 \in A$ and $B(A \cap X)$ does not appear in Supp(Q), or $1 \neg\in A$ and $B(A \cap X)$ does appear in Supp(Q). In either case we have $S(A \cap X) \subseteq \text{Supp}(E)$, contradicting our assumption that no S(C) where $\#(C) \leq t$ appears in Supp(E). **QED.**

Lemma 4. *Suppose that $l \leq 2k$. Then the pirate who attempts to erase information about the origin of $P + F_1$ by adding to it various $\chi(B(A))$s must add on all $\chi(B(A))$ such that $1 \in A$ and $\#(A) \leq [l/2]$.*

Proof. The proof is by induction on the size of A. First, suppose that $A = \{1\}$. The pirate must add $\chi(B\{1\})$ to $P + F_1$. For he must remove $\chi(S\{1\})$ from $P + F_1$, since, if it were left in, the fact that $S(\{1\})$ is contained in $\text{Supp}(F_1)$ but in no other $\text{Supp}(F_i)$ would tell the owner that that the pirate had had access to copy 1. But, since $S(\{1\})$ is contained in $B(\{1\})$ and no other B(A), the pirate has no way of knowing which elements of $B(\{1\})$ are in $S(\{1\})$ and which aren't. Thus the only way the pirate can remove $S(\{1\})$ is by adding $\chi(B(\{1\}))$.

Next, assume that the pirate has added on all $\chi(B(A))$ for all A such that $1 \in A$ and $\#(A) \leq t$, for some $t < [l/2]$. Let $E = F_1 + Q$, where Q is the function that the pirate has added on. We will show that the support of E contains no S(A) such that $\#(A) \leq t$. Clearly, the pirate has erased all $\chi(S(A))$ such that $1 \in A \subseteq X$ and $\#(A) \leq t$. Moreover, he has not added on any $\chi(S(C))$ such that $\#(C) \leq t$. For by Lemma 1 the only way he could have done this would be if $X \cap C = X\text{–}A$, where A is one of the sets of cardinality $\leq t$ such that $\chi(B(A))$ was added on. But this would imply that $\#(X\text{–}A) \leq t$, and hence $l = \#(X) \leq 2t$, which contradicts our assumption that $t < [l/2]$.

The owner can now conclude from Lemma 3 that if $\chi(S(A))$ appears in the support of E, and $\#(A) = t + 1$, then $A \subseteq X$. Moreover, such sets A exist, since $t + 1 \leq [l/2]$ and $l \leq 2k$. Now all he has to do is

take the union of all A such that #(A) = t + 1 and χ(S(A)) appears in the support of E in order to find out which copies the pirate had access to.

Thus the pirate must do something further if he wants to hide the origin of his copy. He has two options. First, he can add on various χ(B(A)) where 1 ϵ A. But he can't add on any χ(B({a})), or the owner will be able to tell, by the appearance of S({a}) in the support of E, that the pirate had access to copy a. However, if he doesn't add on any χ(B({a})), there is some q $\leq$ [l/2] such that no S(A) such that #(A) < q appears in the support E but some S(A) such that #(A) = q does appear. The owner can then use Lemma 3 as before to find the other copies the pirate had access to.

The pirate's other option is to add on some or all of the χ(B(A))s such that #(A) = t + 1 in order to erase some or all of such χ(S(A))s appearing in F_1. But he must erase all such χ(S(A))s since if there was even one that he did not erase, the owner would again be able to conclude, using Lemma 3, that the pirate had had access to every copy a such that a ϵ A. **QED**.

Theorem 5. *Suppose that $l \leq 2k$. Then a pirate cannot erase information about the origin of $P + F_1$ by adding various χ(B(A))s without revealing information about the origins of the other copies he has access to.*

Proof. By Lemma 4 the pirate must add on all χ(B(A)) such that 1 ϵ A and#(A) $\leq$[l/2]. It follows from Lemma 1 and the fact that l $\leq$ 2k that he has also added on all χ(S(X - A)) such that 1 ϵ A $\subseteq$ X and #(A) = $[l/2]$. In other words, he has added on all χ(S(A)) such that 1 ϵ A $\subseteq$ X and #(A) = l -[l/2]. Once again the owner can tell, from the absence of any χ(S(A)) such that #(A) < l - [l/2], that the owner has eliminated all such χ(S(A)). Moreover, once again the owner can use Lemma 3 to can reason that, if any χ(S(A)) such that

$\#(A) = l - [l/2]$ appears in the altered function, then $A \subseteq X$. The owner takes the union of all such A to find $X - \{1\}$. **QED.**

Thus if $2k \geq l$, the pirate cannot erase information about the origin of $P + F_1$ by adding various $\chi(B(A))$s to it without giving away information about the other copies he's obtained. But what if he adds on some $\chi(D)$ where D is a randomly chosen subset of some B(A)? If the pirate were lucky, such a D might contain all or most of the sets S(C) such that $C \cap X = A$ and none or few of the sets S(C) such that $C \cap X = X - A$. This can be made less likely by choosing the sets S(C) large enough so that the chance that such a D would either miss any S(C) entirely (if D is large) or contain an entire S(C) (if D is small) or miss some S(C)s and contain others, (if D is medium-sized) is negligible.

We are thus led to conclude that the fingerprint scheme described above is a $2k + 1$ out of n fingerprint scheme.

The construction of such a fingerprint scheme now seems easy. We simply choose the level of protection we desire and construct the appropriate sets S(A). We are faced with one problem, however: the size of the fingerprints grows exponentially with the level of protection desired. As a matter of fact, since each fingerprint F_i is made up of all S(A) such that $\#(A) \leq k$ and $i \in A$, we have, if $\#(S(A)) = s$ for each such A, that

$$\#(\mathrm{Supp}(F_i)) = s \sum_{j=1}^{k-1} \binom{M}{j}$$

where M is the total number of messages. Thus the size of the fingerprints could easily grow to the point at which they start interfering with the messages.

We can get around the problem of exponential growth somewhat by using several less ambitious fingerprint schemes concurrently. For example, suppose that an owner wishes to protect about 27,000 copies of his message. If he used a 31 out of 27,000 fingerprint scheme, each

fingerprint would take up more than $s10^{50}$ bits. However, suppose that he constructs three 31 out of 31 fingerprint schemes $\{F_1, \ldots, F_{31}\}$, $\{G_1, \ldots, G_{31}\}$, and $\{H_1, \ldots, H_{31}\}$. Each of these three fingerprint schemes takes up

$$s \sum_{j=1}^{14} \binom{31}{j} \approx s10^9$$

bits per fingerprint. Such fingerprint schemes will still take up a relatively small amount of space in something as large as a digital TV show. (If this number is still considered unmanageably large, the owner could instead construct, say, three 13 out of 31 fingerprint schemes, each of which would take up about s200,000 bits per fingerprint, as opposed to a 13 out of 27,000 fingerprint scheme, which would take up about 10^{20} bits per fingerprint.) The owner divides his distribution area into 31 geographic areas, each with 31 outlets selling 31 copies each. The ith copy in the jth outlet in the kth geographic area is fingerprinted by $F_i + G_j + H_k$. Thus if a pirate obtains all his copies from one outlet and attempts to erase the fingerprints we know exactly which copies he has obtained, if he obtains copies form different outlets in the same geographic area we no longer know exactly which copies they are, but we know the outlets they came from, and if he obtains copies fom different geographical areas, we know the areas he visited, although we no longer know the individual outlets he obtained the copies from. Even in this last case, however, we still retain some information about the individual copies. Suppose, for example, that a pirate obtains copies $P + F_1 + G_1 + H_1$ and $P + F_2 + G_2 + H_2$. The owner who retrieves a tampered-with copy can determine that the pirate must have had access to at least two copies of the form $P + F_{i_1} + G_{j_1} + H_{k_1}$ and $P + F_{i_2} + G_{j_2} + H_{k_2}$ where $\{i_1,i_{2,}\} = \{j_1,j_{2,}\} = \{k_1,k_{2,}\} = \{1,2\}$, as shown in the following graph.

H_1				H_2			
G_1		G_2		G_1		G_2	
F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2

Thus he knows there are only eight possibilities for the origins of the two shows.

We have written largely in terms of discrete messages, i. e., messages with finitely many symbols taken from a finite alphabet. But it is clearly possible to do something analogous with continuous messages. A reader who deals with these matters can fill in the details in the obvious way.

NSA Grant MDA 904-83-H-0002 partially supported this work.

References

1. Neal Wagner, "Fingerprinting," *Proceedings of the 1983 Symposium on Security and Privacy*, pp. 18-22, IEEE Computer Society, Oakland, CA, April 25-27, 1983.