On the relation of error correction and cryptography to an off line biometric based identification scheme

George I. Davida* Yair Frankel†
Brian J. Matt‡ René Peralta §

November 29, 1998

Abstract

An off-line biometric identification protocol based on error correcting codes was recently developed as an enabling technology for secure biometric based user authentication. The protocol was designed to bind a user's iris biometric template with authorization information via a magnetic strip in the off-line case while reducing the exposure of a user's biometric data. In this paper we give an in depth discussion of the role of error correcting codes in the cryptographically secure biometric authentication scheme.

An Iris scan is a biometric technology which uses the human iris to authenticate users [BAW96, HMW90, Dau92, Wil96]. This technology produces a 2048 bit user biometric template such that any future scan of the same user's iris will generate a "similar" template. By similar, we mean having an

*Center for Cryptography, Computer, and Network Security, University of Wisconsin-Milwaukee, USA. E-mail: davida@cs.uwm.edu.

†CertCo LLC, New York, NY, USA. E-mail: yfrankel@cs.columbia.edu.

‡Sandia National Laboratories. E-mail: bjmatt@sandia.gov. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

§Center for Cryptography, Computer, and Network Security, University of Wisconsin-Milwaukee, USA. E-mail: peralta@cs.uwm.edu

acceptable Hamming distance within a predefined range, usually around one to ten percent of the size of the code (e.g., Hamming distance between original reading and future reading is set to be in the range from 20 to 200). One can think of a biometric reading of a user as a faulty communication channel which may introduce a limited number of errors. Moreover, the Hamming distance for the biometric readings of two different users has been shown to be much higher, about 45 percent (or 920 bits).

Recently, a cryptographically secure mechanism for off-line biometric identification based on majority decoding and error correction codes (ECC) was developed [DFM98]. The process of an off-line biometric system is the following. A user, during an initialization step, is provided with a storage device / token (e.g., a magnetic strip, smartcard, etc.) by a trusted authorization authority. The token contains a signature and other data which can later be used to prove that the user's biometric is cryptographically bound to the signature of the trusted third party. During a future reading, the user first provides the token to a reader, the reader then obtains a new iris scan template from the user, and finally the reader determines if the new scan is cryptographically bound to the signature (of the trusted authority) on the card. It should be noted that the purpose of the signature is to enable the verification process to be done off-line, i.e. without connectivity to the trusted authority during future verifications. Moreover, it should be observed that the system must handle differences (within the allowed Hamming distance) from the original reading and future readings of the user's iris scan, because the digital signature verification will fail if there is any differences from its original input (message). Off-line biometric authentication protocols, of course, can be used in an online mode by replacing the token entry as a record on an online database.

A biometric identification system which provides the user's biometric template in the clear may not be acceptable to the user, because template could be used for unacceptable purposes if the template is obtained by an unauthorized individual. For instance, an iris scan may be used for medical purposes by an insurance company instead of the legitimate identification process the user was told to submit to.

In the work [DFM98], the feasibility of protecting the privacy of a user's biometric on an insecure storage device was studied. It was suggested that providing additional privacy for the user's biometric may provide for stronger user acceptance. An additional constraint to make the system scalable was

that neither the user nor the reader have private keys (or passwords) when the user must have authorization amongst multiple readers and when password protection is inappropriate. Providing for authorization bound to a biometric template appears to be inherently difficult in this model, because the user's biometric template cannot exist in the clear on the storage device. Since the original template is not stored on the token, a new verification algorithm, different from measuring Hamming distance from original template to new reading, had to be developed.

Here we study the relation of error correction and cryptography to an off-line biometric based identification scheme presented in [DFM98]. In particular, we will study the role of majority decoding, along with algebraic decoding, in the authentication scheme.

1 Background

1.1 Error correcting codes

Majority decoding: In the rest of the paper, we will consider only binary error correcting codes. We will denote by $a||b$ the concatenation of two strings a,b.

Let $\vec{v_i} = v_{i,1}||v_{i,2}||\ldots||v_{i,n}$ be n bit code vectors. Given odd M vectors $\vec{v_i}$, a majority decoder computes vector $\vec{V} = V_1||V_2\ldots||V_n$, where $V_j = \text{majority}(v_{1,j},\ldots,v_{M,j})$, i.e., V_j is the majority of 0's or 1's of bit j from each of the M vectors. We shall use majority decoding primarily to get the best biometric reading possible, thus reducing the Hamming distance between successive $final$ readings $\vec{V}$.

In the biometric authentication protocol, described in Section 1.2 the biometric being measured will be estimated by sampling since the actual unique iris is not measured with precision. The samples that are taken of the iris will converge to the actual unique individual biometric, with majority decoding, with high probability.

Algebraic decoding: An $[n,k,d]$ code [Ber68, MS78, PW88] is a code of n bit codewords (vectors) where k is the number of information digits and d is the minimum distance of code. Such a code can correct $t = (d-1)/2$ errors.

Note: Bounded distance decoding: In the rest of the paper, we assume that the decoding performed at the point of verification is to correct at most $(d-1)/2$ errors. This is necessary to ensure that no bogus biometric is decoded into a valid one. Bounded distance decoding can be readily implemented through a simple count of the Hamming weight of the error vector computed. In some decoding schemes, the error locations that are computed are the roots of some polynomial $\sigma(z)$ over $GF(2^m)$ of degree $t' = degree(\sigma(z))$. If $t' > t = (d-1)/2$ then the biometric is rejected.

1.2 An off-line biometric system

The basic idea of [DFM98] is that a user's biometric template can be used as the information bits of an error correcting code. Now instead of including the biometric template on the storage device, only the error correction bits are necessary. Since only the check bits are stored on the user's card, the available information about the biometric template is reduced. On the other hand, the reader can take a new reading of the user's biometric template, append the error correcting bits, remove the errors using bounded distance decoding, and finally reproduce the original template, which can be verified with the signature on the token.

One other hurdle has to be overcome to provide security. The signature may itself leak the user's template. Observe that $\langle M, \mathrm{SIG}(M) \rangle$ is a signature for message M which leaks all bits of M, yet is a valid signature of M. To resolve this problem, special hash functions were used.

Here is a brief summary of the basic off-line biometric protocol presented in [DFM98].

System Setup: The authorization authority generates its public and private keys and disseminates its public key to the biometric readers. The system also sets up an algebraic $[n, k, d]$ code. We remind the reader that we use bounded distance decoding.

User Initialization: To register, M biometric templates of length k are independently generated for the legitimate user. Majority decoding is then applied to the M biometrics to obtain the user's k bit template $\vec{T}$. Given the k information digits $\vec{T}$, an n digit codeword $\vec{T}||\vec{C}$ is constructed, where $\vec{C}$ are the check digits, in the $[n, k, d]$ code defined at system setup. A storage device is constructed with the following information:

1. Name of the individual, NAME.
2. Other public attributes ATTR, such as the issuing center and a user's access control list.
3. The check digits $\vec{C}$, of the biometric.
4. Sig(Hash(NAME, ATTR, $\vec{T}||\vec{C}$)) where Sig(x) denotes the authorization officer's signature of x, and Hash($\cdot$) is a partial information hiding hash function [Can97] (e.g., Sig(Hash($\cdot$)) is a content-hiding signature) or a random oracle (See [BR93]).

Biometric verification process: When a user presents herself/himself and the card with the information described above, M biometric templates are independently generated for the user. Majority decoding is applied to the M biometric vectors to obtain the user's k bit template $\vec{T}'$. Error correction is performed on codeword $\vec{T}'||\vec{C}$ to obtain the corrected biometric $\vec{T}''$. The signature Sig(Hash(NAME, ATTR, $\vec{T}''||\vec{C}$)) is then verified. Successful signature verification implies the user passed the identification step. For simplicity of exposition, we assume that occasional rejection of a valid user is acceptable (the user would simply repeat the scan). In applications where rejection of a valid user is not acceptable, the parameters of the system can be changed so that such an event has negligible probability. Determining the correct parameters in such a case involves bounding the area under the tail of a binomial distribution (or a Normal approximation to the binomial distribution via the Central Limit Theorem).

Proof of security and in particular the choice of hash functions were discussed in [DFM98]. We now discuss how majority decoding will provide for enhancement to the system.

2 The role of Error Correction

Error correction is performed at two crucial points in the scheme described: The majority decoding at the point of biometric template generation (when the user token is generated) and at the point of verification, when the user presents herself and the token is issued by an authorization center.

To help understand the role of error correction at the various points in the process, we need to consider the probability of per bit error in a measured

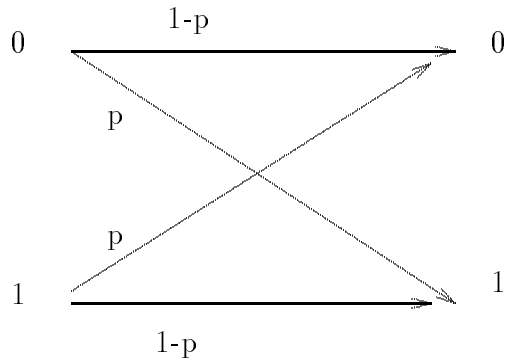

Figure 1: A Binary Symmetric Channel

iris. In [Dau93], the probability of mismatch in each corresponding bit of two samples from the same person, taken at different times, was found to be 0.084, while the probability of a mismatch of corresponding bits of iris scan for two different individuals was found to be 0.45, i.e. about one in two, approaching a random toss of a coin. In addition, each bit of the iris scan appears to be a random variable over a population of different individuals. The errors in the measurement of one individual have been found to be independent over the entire iris scan. Thus one can view errors in the measurements as a binary symmetric channel (see Figure 1).

With this important assumption, which has been empirically validated ([Dau92],[Dau93]), it is possible to apply error correction at the point of acquisition of the iris code. One possible error correction that can be applied is majority decoding of M samples taken at the time of enrollment (or verification). Applying majority decoding at the time of acquisition of the iris scan, one obtains a "reference" iris scan for which we then compute a set of check digits that can correct t errors in the iris scan using an $[n, k, d]$ error correcting code. We note that the check digits, which will be stored on the user's card, will not have any errors in them when error correction is performed. Thus all the t errors that the ECC will correct will come from the k bits of the iris scan, namely the information bits of the error correcting code.

At the point of verification, the user presents herself and the data from, say, a magnetic card, containing the check digits that will be used in correct-

ing a (possibly) erroneous iris scan vector. We now consider the method of acquiring the iris scan at the point of verification.

With majority decoding, using M samples per bit, the probability of an error in each bit then is

$$Prob(M/2 \text{ or more errors}) = P_e = \sum_{i=M/2}^{M} \left(\begin{array}{c} M \\ i \end{array} \right) p^i q^{M-i} \qquad (1)$$

What we are interested in is $n * P_e$, the expected number of errors in a final biometric. Let M_r and M_v be the sampling rates at registration and verification times, respectively. Let P_{e-r} and P_{e-v} be the expected final per bit error rates of the biometric at registration and verification times, after majority decoding. Note that P_{e-r} and P_{e-v} decrease as M_r and M_v increase, respectively. To protect against t errors at verification time, then we choose M_r such that

$$n * P_{e-r} < 1$$

For verification time, we choose M_v such that

$$n * P_{e-v} < t$$

When we compute the check digits C, they are stored on the user's card. The check digits protect against t errors when the biometric is read at the verification point. Observe that t cannot be too large (i.e. if we were to correct, for example, 32 percent errors in the 2048 vector, then we risk accepting an imposter). In fact, for reasons of space efficiency we need to reduce the error rate to something that does not lead to substantial expansion of the data on the storage device carried by the user. In addition, for computational efficiency the ECC needs to be reasonably fast at the point of verification.

At the verification point we consider the cases:

1. The presenter is authentic.
   In this case, the biometric read, using M_v samples to compute the final biometric, should result in $n * P_{e-v} < t$ errors. The errors are then corrected using the C check digits from the user's card. If the biometric has more than t errors, it is rejected.

2. The presenter is an imposter.
   Empirical data shows that the average Hamming distance between imposters and authentics is almost $n/2$. Thus an imposter's biometric

presented for correction, along with C will be rejected with high probability, since the ECC will correct at most t errors.

The error rates in the biometric and the error correction capability of the ECC are critical to secure biometric computation. Using majority decoding, we stabilize the biometric at both the registration point and the verification point to allow the correction of the biometric at the verification point to a reference value. We control the errors corrected at the verification point to achieve the most efficient computation at the verification point, since that is where delays can be problematic.

3 Artificial Iris

While it is believed that artificial devices will not likely succeed at the present time, this may not be the case in the near future, as lcd devices improve in density, color accuracy and other features. If an artificial iris is feasible, then we need to consider defending against one.

Consider an artificial iris that targets one individual. Also, assume that the artificial iris can get as close as distance d_a to a target. In such a case we choose M_r, as before, such that

$$n * P_{e-r} < 1$$

and choose M_v such that

$$t < \frac{d_a - s}{2}$$

where s is a security parameter chosen to make the probabilities of false positives and false rejections acceptable.

4 Concluding Remarks

The role of error correcting codes in reliable, secure and authenticated communication and applications ranging from identification to electronic commerce is an important one. Already there is a significant amount of work, such as the McEliece public key cryptosystem, the Shamir threshold key sharing and the Davida-DeMillo-Lipton key sharing, that has been a link

between the two seemingly separate areas of coding theory and cryptography. This work combines the two to present an identification system that facilitates the use of non-invasive biometrics using an off-line identification scheme that is secure and reliable. Error correction is an important part of this work. Without *ECC* this work would have been more difficult. For example, in the schemes implemented in online systems where a user database of biometrics is stored, the systems are slow even for a moderate number of users. If the number of users is large, in the millions, earlier schmes may very well be too slow for many applications.

References

[BAW96] F. Bouchier, J. S. Ahrens, and G. Wells. Laboratory evaluation of the iriscan prototype biometric identifier. Technical Report SAND96-1033, Sandia National Laboratories USA, April 1996.

[Ber68] E. R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, 1968.

[BR93] M. Bellare and R. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computers and Communications Security*, 1993.

[Can97] R. Canetti. Towards realizing random oracles: Hash functions which hide all partial information. In *Advances in Cryptology. Proc. of Crypto'97*, pages 455–469, 1997.

[Dau92] J. Daugman. High confidence personal identifications by rapid video analysis of iris texture. In *IEEE International Carnahan Conference on Security Technology*, pages 50–60, 1992.

[Dau93] J. Daugman. High confidence personal identifications by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11):648–656, November 1993.

[DFM98] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *1998 IEEE Symposium on Security and Privacy*, pages 148–157, 1998.

[HMW90] J. P. Holmes, R. L. Maxell, and L. J. Wright. A performance evaluation of biometric identification devices. Technical report, Sandia National Laboratories, July 1990.

[MS78] F. J. MacWilliams and N. J. A. Sloane. *The theory of error–correcting codes*. North – Holland Publishing Company, 1978.

[PW88] W. W. Peterson and E. J. Weldon. *Error Correcting Codes*. The MIT Press, 1988.

[Wil96] G. O. Williams. Iris recognition technology. In *IEEE International Carnahan Conference on Security Technology*, pages 46–59, 1996.