Towards a Biometric Random Number Generator – A General Approach For True Random Extraction From Biometric Samples

Daniel Hartung
daniel.hartung@hig.no

Knut Wold
knut.wold@hig.no

Kalman Graffi
graffi@mail.upb.de

Slobodan Petrovic
slobodan.petrovic@hig.no

Abstract: Biometric systems are per definition used to identify individuals or verify an identity claim – one difficulty of getting reliable decisions is the inherent noise that makes it difficult to extract stable features from biometric data. This paper describes how biometric samples can be used to generate strong random numbers which form the basis of many security protocols. Independent from the biometric modality, the only requirement of the proposed solution are feature vectors of fixed length and structure. Each element of such a feature vector is analyzed for its reliability – only unreliable positions, that cannot be reproduced coherently from one source, are extracted as bits to form the final random bit sequences. Optionally a strong hash-based random extraction can be used. The practicability is shown testing vascular patterns against the NIST-recommended test suite for random number generators.

1 INTRODUCTION

One observation with biometric systems is that they deal with noisy physiological or behavioral data. Another observation is that the extraction of reliable features, which allows to discriminate between imposter and genuine attempts, is usually a non-trivial and difficult task. Both observations contribute to the motivation of this work. The common strategy in a biometric system is to extract a compact representation that includes only the most stable, reliable and distinctive information from the raw sensorial data.

On the other hand cryptographic protocols are used more and more widely in nowadays everyday applications as e.g. authentication in online banking. One major building block of those protocols is the proof of freshness. Such a proof is usually done by inserting a cryptographic nonce – a freshly generated random number that is only used once – in a message, which makes a simple message replay detectable. Such random numbers have to be unpredictable for an attacker in order to not compromise the whole protocol. Therefore strong random number generators are needed. The sources of true randomness are often physical processes while randomness from deterministic and highly non-chaotic systems like computers is often very limited. One example of a security protocol using a biometric transaction authentication with the need for strong random numbers for enrollment is the BTAP [HB10, HB11].

In this paper, we present and evaluate the idea to use physical, biometric data to generate strong random numbers. This paper investigates how to combine biometric feature extraction

and random number generation , how to generate the random numbers and how to verify the claimed randomness properties. Simulation results are presented before the paper concludes.

1.1 Noise and Biometrics

Noise is inherently existent in biometric data – data from alive individuals. The term biometric noise is not yet clearly defined and it is often used to describe the variability in the signals due to changes in the biometric (e.g. dirty or torn off finger tips in fingerprint systems, different hair style in face recognition systems), inaccuracies of the sensorial subsystem (e.g. camera noise, dust on fingerprint sensor, pose towards camera), or varying environmental conditions (e.g. lighting, humidity). Here, we use these variations and the noise to generate random sequences.

1.2 Vein Patterns

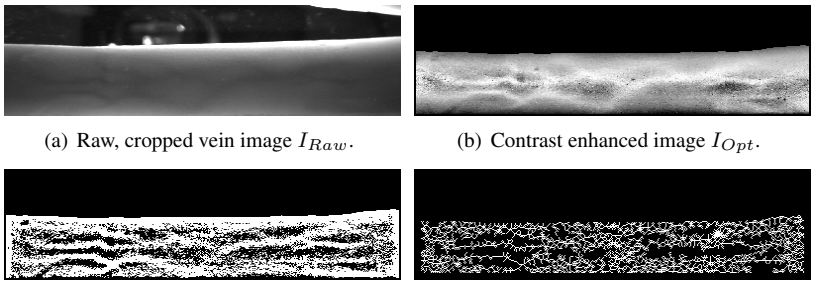
Vein patterns evolve during the embryonic vasculogenesis and their final structure is mostly influenced by random factors [EYM$^+$05]. Even identical twins can be distinguished. The pattern is available at every healthy human, making it an interesting research objective. Commercial applications evolved out of this research, nowadays many ATMs in Japan and Brazil are secured using this biometric modality. The patterns are commonly extracted from images of the palm, the back of the hand or fingers. The International Biometrics Group (IBG) 6th report 2006 confirms recognition rates fairly at the same level for two different vein and one iris-based authentication system [Int06]. An interesting aspect of vein recognition is the fact that the information is not visible, it is hidden inside the body. Unlike fingerprints it is not possible to leave a vein pattern representation unintentionally in public places and thus it is not possible for an attacker to acquire the pattern in daily life or to replicate it. Furthermore there is no relation to criminal prosecution.

The imaging approach makes use of the absorption capacity of particular substances in the blood running through the veins. To capture the image, the region of interest is illuminated with a near-infrared (NIR) light source with wavelengths around 700 to 1,000 nm. A reflection or transmission technique can be used. Deoxygenized hemoglobin highly absorbs rays within this wavelength band while the surrounding tissue does not. NIR-sensitive optical sensors are used to capture the image of the vein pattern.

1.2.1 Feature Extraction Examples

The following images will be used during later stages of the random extraction: figure 1(a) shows an example vein pattern image and a STRESS [Øyv11] contrast enhanced version in Fig. 1(b), its segmented version in Fig. 1(c) produced using a local thresholding algorithm. The image is then transformed to a skeleton representing the topology of the vein pattern (Fig. 1(d)) by using morphological operators. The database consists of 10800 finger vein images from all 10 fingers of 45 data subjects acquired in 12 sessions, each image having a size of

111×401 pixels. Throughout the paper only the left middle fingers will be considered.



(a) Raw, cropped vein image I_{Raw}. (b) Contrast enhanced image I_{Opt}.

(c) Segmentation of a vein pattern image I_{Seg}. (d) Skeletonization of segmented image I_{Skl}.

Figure 1: A sample finger vein image and its representations within the pipeline. Note: an unstable segmentation and skeletonization method was chosen.

2 BIOMETRIC RANDOM NUMBER GENERATOR

2.1 Random Number Generation

Random numbers have various important applications in computer science, from computer simulations, statistical sampling to cryptology. This section will describe some properties of randomness and the general classification into two distinctive classes: True random number generators (TRNG) are based on measurements of physical processes that are expected to be random like coin flipping, chemical processes including radioactive decay and atmospheric radio noise or processes based on quantum mechanics. Pseudo random number generators (PRNG) are based on deterministic computations where the output is predictable, but initialized with a true random seed or key makes the PRNG output difficult to predict.

In order to verify the before mentioned and additional properties, statistical tests can be performed on random numbers. The NIST suite "A Statistical Test Suite for Random and Pseudo random Number Generators for Cryptographic Applications" based on [And] is a complete and commonly used test suite. It will be the basis for the evaluation of the generated random numbers in section 3.

2.2 State of the Art

Very limited work has yet been done on the field of biometric random generation. During the literature search only a hand full of papers was focusing on biometric random number generation. Often the terms were used incorrectly, in [CRNF06], the title indicated a random key generation from iris data, instead the extraction of non-random keys from the same biometric trait was discussed, related to a biometric key release or extraction. The research work in [KvM07] was focusing on the sources of randomness in mobile devices, focusing on

Source	Entropy (bits)
I_{Raw}	25165
I_{Opt}	26930
I_{Seg}	19211
I_{Skl}	8003

Table 1: Entropy estimation for the different stages of the pipeline.

hardware sensorial noise from the camera or the microphone, not considering the use of the built-in sensors as sensors for biometric traits like voice or face recognition.

The work in [SWA$^+$04], was closest to the scope of this paper. In there, the use of biometric data in the medical sense – in example animal neurophysical brain responses and human galvanic skin responses – were examined as sources of randomness. An approach was used, where physical measurement data was binarized and the last fluctuating digit was used as random bit sequence over time. Their true random generator passed successfully the NIST test suite as well as other statistical tests, whereas the brain signals come along with complex data measurement and the skin response did not show a sufficiently fast sampling rate.

Basis for the verification of the approach presented in this paper is a subsection of the database described in section 1.2.1.

2.3 Entropy Estimation

Entropy is an important measure in random number generators to estimate the quality of randomness. The amount of information – or entropy – H, that can be extracted from K occurrences, each having the probability p_i with $i = 1, 2, ..., K$ can be computed using the Shannon-Entropy:

$$H = -\sum_{i=1}^{K} p_i \cdot log_2(p_i), \tag{1}$$

In practice the probabilities are not known, the concept of the maximum-likelihood estimator $\hat{p_i}$, that estimates the probabilities by using absolute frequencies n_i over N observations, can help out. Where occurrence i is approximated with: $\hat{p_i} = n_i/N$. The resulting formula is given by:

$$\hat{H} = -\sum_{i=1}^{K} \hat{p_i} \cdot log_2(\hat{p_i}) \tag{2}$$

The entropy is estimated for our test database, the average entropy of the skeletal vein images is given in Table 1, not considering the correlation between the single pixels. That means according to the estimator theoretically about that many bits of information can be extracted in average from one vein pattern image. A more refined estimation for the biometric entropy in finger vein images is currently under development and will be published soon.

2.4 Image Based Biometric Random Number Generation (BRNG)

Having discussed the motivation and requirements for a biometric random number generator, next, we present our approach for a BRNG. Data from different stages of a biometric pipeline are used as input to the proposed BRNG. The generic approach only requires a fixed length and a fixed structure of the feature vector. Here we will use images from the vein patterns, every other kind of features would also work. In order to find the most appropriate stage of the feature vector, first the raw image itself (I_{Raw}), followed by an enhanced and contrast optimized image is taken into account (I_{Opt}). After that the segmented and binarized representation (I_{Seg}) is considered as well as the skeletonized version (I_{Skl}).

The idea is that lower level features (in earlier stages of the pipeline) yield higher degrees of noise e.g. from the sensor, and recent work shows that using the Photo-Response Non-Uniformity (PRNU) of sample images the imaging sensors can be distinguished [FFG08]. The randomness in higher level features is more and more based on the biometric information since unnecessary information is being removed during the preprocessing steps. One assumption is that these features have a better statistical quality and are more difficult to predict even though the amount of information in the images is reduced. The **hypothesis** that is tested later on: low level features produce lower quality random sequences than higher level features.

All real-valued feature vectors or images can be binarized using the interclass mean image ($\bar{I}$) of a training set (one / two dimensional case). One advantage of the binarization is that the amount of ones and zeros is approximately equal. The bit value $I^{Bin}(x, y)$ of every pixel $I(x, y)$ at position (x,y) in the source image I is computed as:

$$I^{Bin}(x,y) = \begin{cases} 0, & \text{if } I(x,y) < \bar{I}(x,y) \\ \\ 1, & \text{if } I(x,y) \geq \bar{I}(x,y) \end{cases} \tag{3}$$

Note the feature vector F is derived as concatenation from the image I's columns:

$$F = [I(1,1), I(2,1), \ldots, I(end,1), I(1,2), I(2,2), \ldots, I(end,2), \ldots, I(end,end)] \tag{4}$$

The binarized feature vector F^{Bin} is derived from I^{Bin} in the same way.

During the next step of the BRNG, every position in the feature vector F – which is defined in Equation 4 – is analyzed for its reliability, meaning that single positions can be reproduced very accurately over many captures. The idea is based on work from Tuyls et al. [TG04], where the helper data scheme (HDS) is introduced that combines cryptography with biometrics to secure the privacy and the templates. Following this approach we could use the same mechanism used there to estimate the reliability of positions in the feature vector to estimate the inverse, the least reliable positions, and to use those bits for our random sequence. Using the inverse measure, we can select positions that are not reproduced accurately over many captures and that are being close to the mean value used for the binarization, resulting in random and flipping bits.

Reliability $R(i)$ (data subject specific) on position i of a fixed length and structured real-valued feature vector F, in the context of the HDS is estimated using the fraction of the inter-class

var_{inter} and the intra-class var_{intra} variance:

$$R(i) = \frac{var_{inter}}{var_{intra}} = \frac{(F(i) - \overline{inter}(i))^2}{(F(i) - \overline{intra}(i))^2}, \tag{5}$$

using the mean value of the class $\overline{intra}$ (calculated from a fixed number of samples of the same biometric trait – called training set) and the mean value of the whole population $\overline{inter}$ (mean of all training sets together).

Here we introduce the unreliability measure:

$$U(i) = \frac{1}{R(i)}. \tag{6}$$

Border zones in the image that are always set to zero or one are resulting in high values for U, since they are very close to the inter class mean. Those positions are not interesting for the bit extraction since they are constant over the samples and occur in blocks, therefore $U(i)$ is set to zero for those positions.

In order to make an extraction of bits more efficient the indexing vector U_{idx} contains the indexes i sorted in descending order of $U(i)$.

A variable $\kappa < |F|$ is introduced to define the amount of unreliable bits that are to be extracted from and used for the random sequence Δ:

$$\Delta = [F(U_{idx}(1), F(U_{idx}(2)), \ldots, F(U_{idx}(\kappa))], \tag{7}$$

A further degree of freedom is given when using the help of a hash function h as a random extractor. Depending on the needed length of the random bit vector and the quality of randomness a variable λ is introduced splitting the random sequence Δ into k chunks C_i of length $\lfloor \kappa/\lambda \rfloor$. If λ is set to one, the whole sequence is used as input to a hash function, the larger it gets, the more chunks are created. Each chunk itself can be used to create a new hashvalue $h(C_i)$. The length of each chunk C_i should be larger or equal to the output length of the hash function.

$$\Delta_h = [h(C_1), h(C_2), \ldots, h(C_k)]. \tag{8}$$

The final sequences Δ and Δ_h are xor-ed with its inverse order version to enhance the distribution of biased features, since mainly positions containing logical zeros are selected as most unreliable bits.

3 SIMULATIONS

The simulations cover the statistical test of NIST based on the data that was extracted as described in section 2.1. The database was divided into two distinct sets each containing 540 samples – 12 samples from 6 sessions of each of middle left finger of 45 data subjects: the odd numbered sessions are taking as training set and the even numbered ones for verification.

Source	κ	λ	Length Bitstream	# Bitstreams	Result
I_{Raw}	25165	x	135000	100	5.6%
I_{Raw}	25165	157	135000	100	87.9%
I_{Raw}	25165	78	67000	100	93.4%
I_{Opt}	26930	x	145000	100	69.3%
I_{Opt}	26930	168	145000	100	98.2%
I_{Opt}	26930	84	72000	100	98.2%
I_{Seg}	19211	x	100000	100	66.9%
I_{Seg}	19211	120	100000	100	98.1%
I_{Seg}	19211	60	50000	100	97.2%
I_{Skl}	8003	x	43000	100	1.4%
I_{Skl}	8003	50	43000	100	95.3%
I_{Skl}	8003	25	21000	100	97.9%

Table 2: Experimental results of NIST test suite (standard parameters) applied to the random sequences extracted from the vein database. Hash function used: SHA-1. x = no hashing. Result: ratio of how many of the NIST tests successfully passed.

In order to run the NIST test suite several Mbit of data are needed, therefore the resulting random sequences will be concatenated and presented to the test suite. The maximal amount of unreliable bits κ extracted from the various samples is set to the estimated entropy value from table 1.

3.1 NIST Results

The unreliable bits from the raw images are not qualified for the random extraction, but after a strong random extraction using a hash function very good NIST test results are achieved. With more than 95% of successfully passed tests, hashed unreliable bits from higher level features (I_{Opt}, I_{Seg} and I_{Skl}) are especially qualified. The amount of successfully passed tests is peaking with more than 98% for the hashed unreliable bits extracted from the optimized or segmented images (see table 2). Lower values for λ, resulting in bigger chunks as input for the hash function, are not effective to improve the random properties for higher level features.

4 CONCLUSIONS AND FUTURE WORKS

The results are quite diverse – on the one hand the pure unhashed versions of the data are not useful as a basis for BRNG, as they pass only a minor amount of the tests . On the other hand, good randomness properties are seen in case of the hashed version of all images, in particular higher level images.

The hypothesis cannot be verified; the quality of the random sequence extracted, measured in successful runs over the NIST test suite, is increasing from the raw level to the more abstract ones ($I_{Raw}, I_{Opt}, I_{Seg}$), but the skeletonized features pass only few of the NIST test if unhashed. The influence of hashing on passing the NIST test is too large to claim the hypothesis that abstract biometric information offers a higher entropy and thus better randomness characteristics.

Future works will focus on an improved quality of random bits generated from one biometric sample and on the statistical properties. In addition future research will focus on a more sophisticated model for the biometric finger vein entropy estimation which may lead to quality metric for single samples as well as for capturing devices and feature extraction algorithms.

References

[And] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo. National Institute for Standards and Technology, NIST Special Publication 800-22 Revision 1a. Revised: April 2010,.

[CRNF06] Luis Castañón, MariCarmen Reigosa, and Juan Nolazco-Flores. Biometric-Iris Random Key Generator Using Generalized Regression Neural Networks. In Moonis Ali and Richard Dapoigny, editors, *Advances in Applied Artificial Intelligence*, volume 4031 of *Lecture Notes in Computer Science*, pages 530–539. Springer Berlin / Heidelberg, 2006.

[EYM+05] Anne Eichmann, Li Yuan, Delphine Moyon, Ferdinand Lenoble, Luc Pardanaud, and Chinstiane Bréant. Vascular Development: From Precursor Cells to Branched Arterial and Venous Networks. *International Journal of Developmental Biology*, 49:259–267, 2005.

[FFG08] Tomás Filler, Jessica J. Fridrich, and Miroslav Goljan. Using sensor pattern noise for camera model identification. In *ICIP*, pages 1296–1299, 2008.

[HB10] Daniel Hartung and Christoph Busch. Biometric Transaction Authentication Protocol. *Emerging Security Information, Systems, and Technologies, The International Conference on*, 0:207–215, 2010.

[HB11] Daniel Hartung and Christoph Busch. Biometric Transaction Authentication Protocol: Formal Model Verification and "Four-Eyes" Principle Extension. In *Financial Crypto, 2nd Workshop on Real-Life Cryptographic Protocols and Standardization*, 2011.

[Int06] International Biometrics Group (IBG). *Comparative Biometric Testing Round 6 Public Report*, Sep 2006.

[KvM07] Jan KRHOVJÁK, Petr ŠVENDA, and Václav MATYÁŠ. The Sources of Randomness in Mobile Devices. *In Proceeding of the 12th Nordic Workshop on Secure IT Systems, Reykjavik*, pages 73–84, 2007.

[SWA+04] J. Szczepanski, E. Wajnryb, J. M. Amigó, Maria V. Sanchez-Vives, and M. Slater. Biometric random number generators. *Computers & Security*, 23(1):77 – 84, 2004.

[TG04] Pim Tuyls and Jasper Goseling. Capacity and Examples of Template-Protecting Biometric Authentication Systems. In *Biometric Authentication*, volume 3087 of *Lecture Notes in Computer Science*, pages 158–170. Springer Berlin / Heidelberg, 2004.

[Øyv11] Øyvind Kolås, Ivar Farup, Alessandro Rizzi. STRESS: A new spatial colour algorithm. Journal of Imaging Science and Technology (in press), 2011.