UDK 004.056.55
Original scientific paper

BIOMETRIC CRYPTOGRAPHY AND NETWORK AUTHENTICATION*

Tonimir Kišasondi, Miroslav Bača, Alen Lovrenčić
University of Zagreb, Faculty of organization and informatics, Varaždin, Croatia
{tonimir.kisasondi, miroslav.baca, alen.lovrencic}@foi.hr

Abstract. *In this paper we will present some schemes for strengthening network authentification over insecure channels with biometric concepts or how to securely transfer or use biometric characteristics as cryptographic keys. We will show why some current authentification schemes are insufficient and we will present our concepts of biometric hashes and authentification that rely on unimodal and multimodal biometrics. Our concept can be applied on any biometric authentification scheme and is universal for all systems.*

Keywords: *biometric hash functions, flaws in authentification, identity based encryption.*

1. INTRODUCTION

As we all know storing passwords in plaintext is considered insecure, so cryptographic hashes are used to obsufurcate plaintexts. A cryptographic hash takes a plaintext, and then calculates a hash value from it. Cryptographic hashes should always give unique output for a matching input. That's why they are used for file integrity checking, password hashing and similar applications.

If two inputs for a hash function produce the same output that means the hash has a collision and it is considered insecure. Also, cryptographic hash functions must be irreversible. Most common hash functions today are: MD5, SHA-1, SHA-256, SHA-512 [4], WHIRLPOOL and TIGER.

Hash functions can be "reversed", which means a plaintext can be obtained with bruteforce attacks, rainbow tables [8], CRC tables [3], Modified CRC tables [7]. Also hash functions are "stronger" and harder to break if they obtain a large input, and that is the main concept on which biometric hashes derive their security. Because normal passwords are varied in size and ranges, but most common user passwords are weak and easily defeated with rainbow cryptanalysis. Our concept of biometric hashes has an extremely long input and is nearly impossible to reverse engineer since a brute force attack would be infeasible and a rainbow table would be simply too big.

*Shown results came out from scientific project (Methodology of biometrics characteristics evaluation 016-0161199-1721), supported by Ministry of science, education and sport Republic of Croatia.

2. FAILURE OF CLASSIC HASHES ON MODERN CRYPTANALYSIS

The main failure point of classic password authentification systems is that users commonly use weak passwords of under eight lowercase and uppercase alpha characters with numbers or use phrases that are found in dictionaries [11]. On figure 1 we show how classic tables are correlated to various variables. We assume that the chain number in table will be 40 million, since that is the most practical size of a table, and for example, we will take the MD5 hash[9]. Benchmarks were done on a 1.4 GHz Pentium-M processor, 1Mb L2 cache with 512 Mb Ram, so a cluster system would be more powerful and would take significantly less time while also it could parallelize all actions. On fig. 1 we show the correlation of the input character size (a- for lowercase characters, A for uppercase characters, 0 for numerics), and the length of the password (for example 1-7 for passwords of 1 to 7 characters) Chain length is the rainbow table chain length in the table.

Data set	Password length	ChainLength	Number of tables	Time	Probability of successful cracking (Table size)
a	1-7	4000	1	6,05s	99,11% (610Mb)
a	1-8	4000	1	6,95s	46,59% (610Mb)
a	1-9	4000	1	7,9s	2,77% (610Mb)
aA0	1-8	8000	1000	8,79h	76,34% (596Gb)
aA	1-8	8000	50	26,10m	25,40% (30Gb)
aA0	1-8	50000	300	4.5D	93,26% (178Gb)

Figure 1. Classic Rainbow Table size

As we can see, classic rainbow tables become infeasible with large datasets. This can be softened with the use of our modified CRC tables that use longer processing time to find the hash, but are smaller. Also tables can have longer chain lengths to compress them. This generation can be done on a clustered system, so generating the last example table can be about one month with less than a day of cryptanalysis for any number of hashes. This shows that "weak" passwords, of under 8 characters mixed alpha numerics are trivial to crack and that large passwords, of mixed input sets are extremely difficult to crack and this is the basic concept of biometric hashes.

3. BIOMETRICS, UNIMODAL AND MULTIMODAL BIOMETRIC SYSTEMS

Since we want to use biometric characteristics in our work, we will define some prerequisites for our systems.

The favored biometric characteristic is [6]:

- Fast to process and acquire
- Unobtrusive to the bearer
- Preferably contact-less
- Unique

Also, we prefer the usage of multimodal systems. Multimodal systems are systems that use more then one biometric characteristic to authenticate a user where unimodal systems use only one characteristic. Also the characteristic must have a distinct output that can be

used for a biometric hash, or we must be able to create an eigenvector. This means that the output can be similar to a password, and thus can be compared in hashed form. The other variant is that we transfer and store / use biometric characteristic in encrypted form with stronger asymmetric cryptographic algorithms like RSA or ElGamal.

4. BIOMETRIC AUTHENTICATION CONCEPT

4.1 ENROLLMENT

First, a person must be enrolled. Enrollment is collecting a persons biometric characteristics, over multiple times so a referent sample can be acquired [1]. For biometric characteristics, several can be predominantly best for biometric authentication, like keystroke dynamics and other variants that can hold a precise value and don't require any special type of conversion for usage. For multimodal authentication, we must obtain all the characteristics that will be used. The more characteristics we acquire, we will have more characteristics we can use for characteristic rotation. The main principle is that we acquire multiple characteristics, and use a fixed number for authentication . For example, if we enroll ten fingers and use two for authentication, which means that each time we can request two different fingers for authentication. This method can reduce and harden attempts with "replay attacks" (for example, if a malicious individual acquires a characteristic and tries to present the acquired characteristic). This method is simple for users, and hardens existing systems. After collection and processing, the templates are stored in a database.

4.2. MODEL FOR BIOMETRIC AUTHENTICATION

Here we can present the concept of the biometric authentication model, based on hash functions on figure 2.

This concept is very easy to comprehend. First off, the system selects a number of biometric characteristics that will be used for authentication. Then we extract features and patterns that we will need for the processing part. Processing part must create a value (like an eigenvalue) that if it's hashed can be uniquely correspondent to the biometric template base. The authentication is done like with any other hash system as shown in Figure 3.

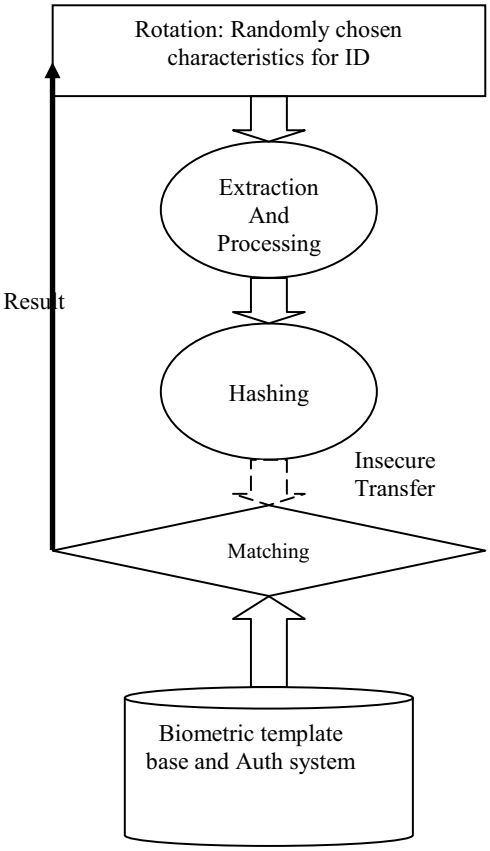


Figure 2. Model for biometric authentification

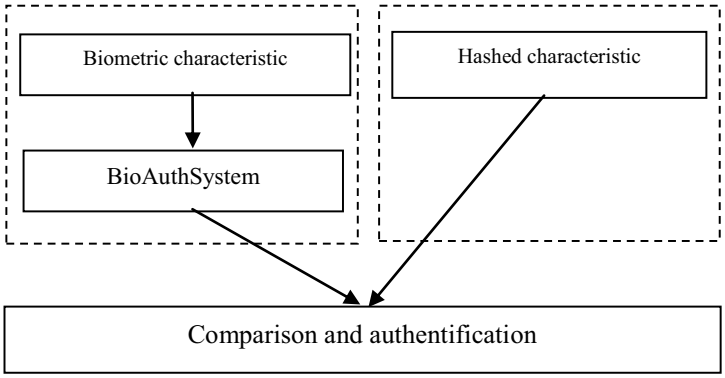


Figure 3. Simple hash authentication

4.3 HOW TO HASH A BIOMETRIC TEMPLATE

As we already said, the principle failure of password systems is the size of the passwords which can be reverse engineered with use of modern cryptanalytic methods. Biometric templates or characteristics are complex and large, and have a uniform distribution. This is a very good quality, since a person who would want to create a CRC, M-CRC or Rainbow table would need a extremely large dataset, and thus a table would be gigantically large. Also, since the biometric characteristic is large, and we will need to utilize multiple rounds of a hash algorithm, and that adds to the complexity of the cryptanalysis.[5]

The other method is to use asymmetric cryptography methods like ElGamal or RSA for transmission of the characteristic. In that method, a biometric characteristic can be signed like any other document or file. Some public key encryption methods have been applied to some Microsoft's USB fingerprint scanners, but it has been shown that those measures can be easily circumvented with USB MiTM like attacks (Replay attacks), Difference attacks and similar measures. If the system would be enabled to send a hash value with a nonce, that problem would be neutralized.

4.4 BIOMETRIC CHARACTERISTIC AS MAIN OR SURROGATE KEY IN CRYPTOGRAPHIC SYSTEMS OR PKI INFRASTRUCTURE

One other concept that can be used is to use the biometric characteristic as a decryption key for the smart card protected certificate or other cryptographic container. Since smart cards utilize cryptography, they are considered "secure". But unfortunately there were successful attempts with timing attacks and smart-cards holding PKI information are considered mostly secure. Also, a biometric characteristic can be used as a key in a cryptosystem. Here we will show some methods that can utilize this concept to strengthen existing cryptographic concepts. The outline of the system is shown in figure 4.

The main feature is to create a cryptographic system that can utilize biometric characteristics as the key. Since we don't want to use a pure characteristic as the key, we can enroll multiple characteristics and use characteristics rotation. After we have a characteristic, we have to hash it so each encodement will be unique and same. This can be done with eigenvectors or is native to some biometric characteristics like typing dynamics. This actually means the biometric hash can be of some arbitrary length like 256 / 512 / 1024 / 2048 bit length and will be used as a symmetric key for our cryptographic container which can be implemented as we wish. After decryption with the biometric hash, we can extract the keypair or a key and use it in a standard encryption algorithm. If we want to use the model to store a certificate, we can also decrypt the certificate with the biometric hash, and the model is slightly changed

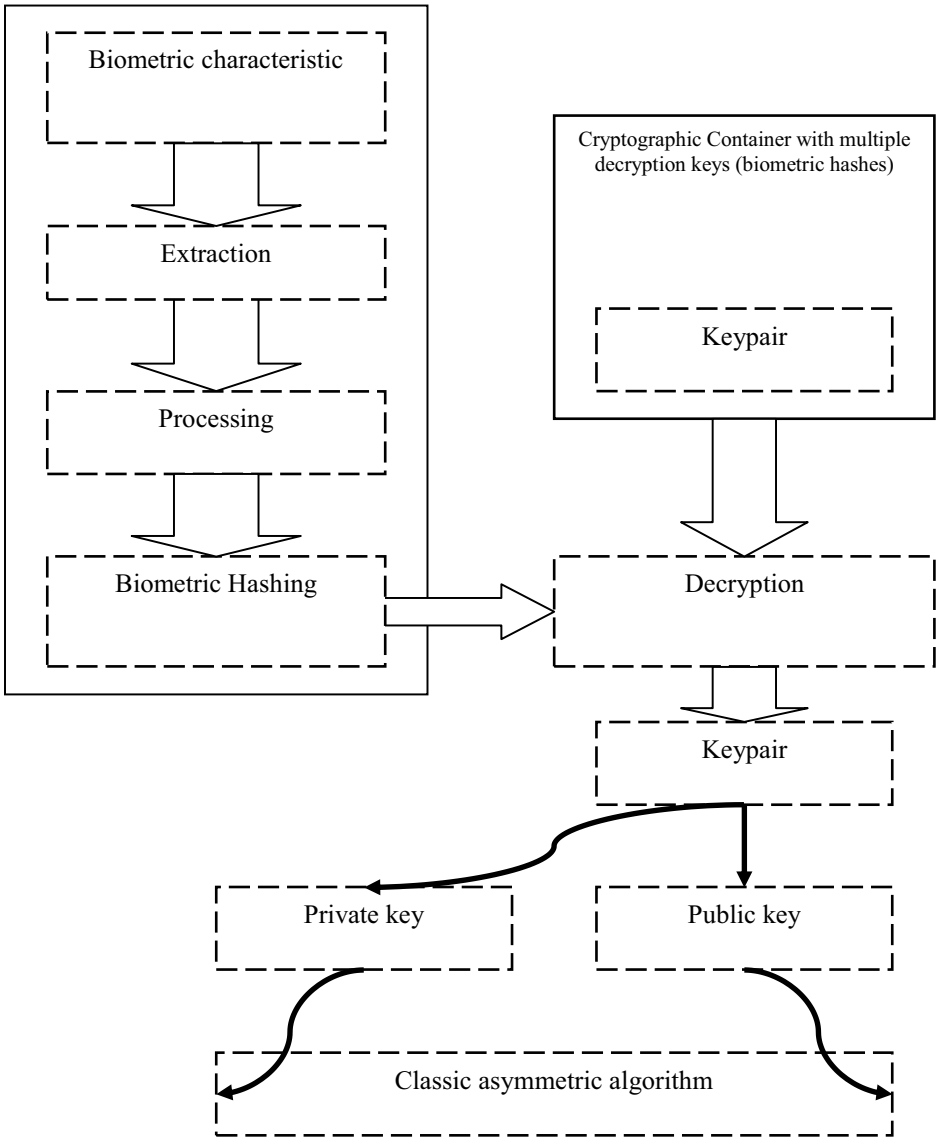


Figure 4. Biometric cryptography model

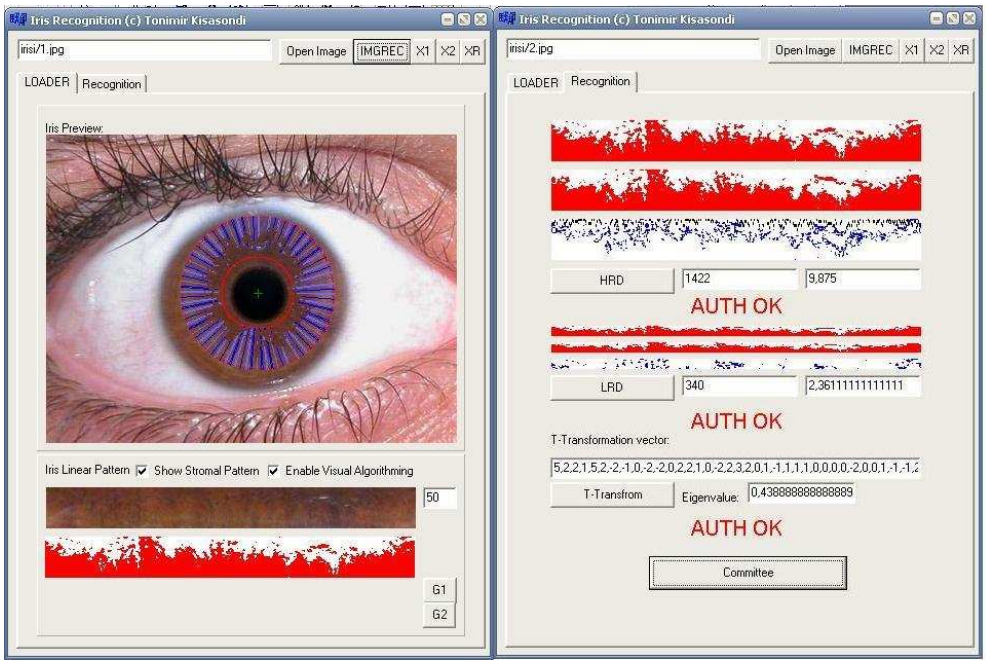
4.5 RESEARCH DATA CONCERNING CHARACTERISTIC ROTATION AND OTHER NEW BIOMETRICS CONCEPTS

Shown results came out from scientific project (Methodology of biometrics characteristics evaluation 016-0161199-1721), supported by Ministry of science, education and sport and we used that data in our research of this paper. From that results we found out that by using our CRC tables, we can effectively crack classic non salted hashes in a extremely short timespan. Also, the main point in trying to implement biometric cryptography is that we cannot effectively protect most of the biometric characteristics because of the simplicity of cracking some fingerprint scanners.

We tried with some characteristic compounds based on silicone-acrylic bases and natural gelatin. We found that silicone-acrylic bases with high moisture compounds can simply crack most modern multispectral optical sensors that rely on skin moisture, papillary lines and subdermal information to identify the person that holds the fingerprint. Since an attacker can simply crack that kind of sensors, with full stealth because the artificial fingerprints are thin (1 to 3 mm), we need to harden the acquire of fingerprints so that attackers cannot use them against the identification system. The simplest form is characteristic rotation that we mentioned earlier.

4.6. IRIS RECOGNITION AS A GOOD CANDIDATE FOR BIOMETRIC CRYPTOGRAPHY

Unlike fingerprints, thermography, hand geometry, facial images and similar non static methods, DNA and iris patterns remain static trough the entire lifetime. Since DNA is hard to extract and is a potential invasion of privacy, iris recognition shows as a promising hard method which is static and cannot be changed [2]. With great FRR and FAR rates for iris recognition it is a promising hard method that can be used in high security applications. Based on previous researches that have stated in common knowledge that the stromal pattern behind the cornea doesn't change in time, and that it can only be changed with physical force, severe illness or damage which would destroy or damage the eye, we can conclude that the iris pattern can be uniquely extracted each time. If the pupil would dilate or contract based on the light, a constant intensity of light at the source can be regulated for scanning (as it is mostly done in some systems). That way a extracted iris pattern can be used in any concept that we shown in this work. In the Picture 1. we show a prototype application that is used in our research.



Picture 1. IRA – Iris recognition

Both stromal patterns from the image come from the same person. As we said, we can use the characteristics in any way that is specified in this work.

5. CONCLUSION

In this paper we have shown some basic concepts that can be used to improve authentication methods like characteristics rotation, biometric hashes [10] and the concept how we can use biometric hashes for cryptographic purposes. Those concepts can be used to improve existing biometric authentication systems as concepts that are easily implemented.

Also, on laptops we checked (Some early IBM T models and HP models with fingerprint readers; we don't have data for never models). We still don't know why vendors haven't implemented characteristic rotation (in example, fingerprint rotation that uses 2 requested fingers for recognition, each time a different random pair.)

Our future research will be concentrated on our biometric X509 certificates, and we will extend the basic concepts that we have shown. Also, with biometric X509, we are developing public key protocols that will use additional biometric authentication of both sides for secure asynchronous and synchronous communication. Since fingerprint readers are cheap, and come on some laptops as standard, and our nearly complete algorithms for iris recognition don't require special hardware, it is possible that the typing dynamics, iris patterns, and fingerprints will be used as part of smart-card, mifare or RFID enabled certificate holders. Also, some preliminary testing with biometric hashes (modified WHIRLPOOL hashes with eigenvalues for iris recognition have shown promise for the usage of the biometrics cryptography.

REFERENCES

[1] Bača, M., Čubrilo, M., Rabuzin, K. (2005): Biometric in ITS security, IIS'05 Conference proceedings of 16th International Conference „Information and intelligent systems", Varaždin, Croatia, pp. 285-291.

[2] Bača, M: Walsh transform in fingerprint minutiae extraction; Information and intelligent systems Varaždin : FOI, 2004.

[3] Davis, J. H. Application of CRCs to TMTO. On-line: <http://www.md5lookup.com/?category=main&page=applications_of_crcs> acquired: 21.5.2006

[4] FIPS PUB – 180-2: SHA-512

[5] Hellman, M.E. (1980): A cryptanalytical time-memory trade off. IEEE Transactions on Information theory IT-26

[6] Hutinski Ž; Bača M: Sigurnost elektroničkog poslovanja i identiteta. 3. Savjetovanje o privatnosti i upravljanju identitetom.

[7] Kišasondi, T., Bača M., Schatten, M : Various aspects of improving computer authentication systems, Conference proceedings of MIPRO 06, ISS section.

[8] Oechslin, P. (2003): Making a Faster Cryptanalytic Time-Memory Trade-Off, Laboratorie de Securite et de Cryptographie (LASEC), Ecole Polytechnique Federale de Lausanne

[9] RFC 1321: The MD5 Message Digest algorithm

[10] RFC 3174: US Secure Hash Algorithm 1

[11] Zalewski, M. Silence on the wire, a field guide to passive reconnaissance and indirect attacks. 2005, No Starch press.

Received: 15 March 2007

Accepted: 19 September 2007