Biometric Cryptosystems vs Traditional Cryptosystems

Mirella Amelia Mioc

Abstract— Since the beginning of civilization, the identification of a person was crucial. Security, government, communication, transportation, health care, finance and others needs to have this person identification as an integral part of the infrastructure. In traditional cryptosystems, user authentication is based on possession of secret keys, but this keys can be stole, forgotten or lost, so providing non-repudiation. Biometric authentication systems based on physiological and behavioral characteristics of a person may replace the authentication component of traditional cryptosystems. A cryptographic key can be bind with the biometric template of a user stored in the database in such a way that the key cannot be used without a biometric authentication. Traditional methods of personal recognition can be used for identification or verification of identity and so obtaining an increasing security and convenience. A brief overview of biometric methods will be presented in this paper.

Keywords—Cryptosystem,Biometrics, Recognition, Verification, Identification, Security, authentication.

I. INTRODUCTION

Biometrics has been used for secure identification and authentication, because biometric data is non-transferable, unforgettable and unique. Nowadays biometrics was replace by Biometric Cryptosystems. Sometimes some of these systems can be integrated with other technologies such as digital signatures or Identity Based Encryption (IBE) schemes results in cryptographically secure applications of biometrics. Some biometric remote authentication schemes designed show that one can improve the database storage cost significantly by designing a new architecture, which is a two-factor authentication protocol. This construction became also secure against the new attacks, which disprove the claimed security of remote authentication schemes. A new construction which combine cancelable biometrics and distributed remote authentication can be build for obtaining a highly secure biometric authentication system.

. Thus, leakage of the secret key of any system component does not affect the security of the scheme as opposed to the current biometric systems involving cryptographic techniques.

Designing a new biometric IBS system can be based on the currently most efficient pairing signature scheme in the literature. The security of such kind of new scheme was proved comparing to existing models for fuzzy IBS, which basically simulates the leakage of partial secret key components of the challenge identity. According with the novel features of this scheme, a new biometric IBE system differs from the current fuzzy systems with its key generation method that not only allows for a larger set of encryption systems to function for biometric identities, but also provides a better accuracy of the users in the system. In this context, can be designed a scheme that allows for the use of multi-modal biometrics to avoid collision attacks. Also the design of biometric IBE systems without using pairings can be developed. The current fuzzy IBE schemes are secure under bilinear assumptions and the decryption of each message requires pairing computations almost equal to the number of attributes defining the user. Thus, fuzzy IBE makes error-tolerant encryption possible at the expense of efficiency and security. The design of a completely new biometric IBE is based on error-correcting codes, generic conversion schemes and weakly secure anonymous IBE schemes that encrypt a message bit by bit. The new developed scheme is highly secure and more efficient comparing to pairing-based biometric IBE.

Mirella Amelia Mioc is with the Department of Computer Science, Faculty of Automatics and Computers, "Politehnica" University of Timisoara, ROMANIA.

II. TEORETICAL BACKGROUND

For proving our identity, we can use three ways:

- Something we have (e.g. a smartcard)
- Something we know (e.g. a PIN code, a password)
- Something we are (biometrics, e.g. fingerprint, face, iris)

Usually, we trust in everyday life, in a combination of both two, meaning something-we-have and something-we-know (e.g. banking cards, SIM card in mobile phones). Everybody knows that a password can be guessed or communicated and a personal device can be borrowed or lost. For bringing high confidence in the authenticated interlocutor an authentication can be build by using a three factor authentication developed with the help of one or several biometric techniques. The advantage of using biometrics in setting a single or multi-factor authentication is that biometric data is always handy, it is no possibility to forget or loose it, so it is not necessary to remember or keep it secret for secure authentication (as in the case of a long password). Usually in Biometrics a user is uniquely defined and is direct evidence of personal participation in authentication, especially when we have a combination of two different biometric traits as it will be called multi-modal biometrics or biometric fusion. Nowadays, many countries collect at least two different biometric traits, as

being face and fingerprint from each traveler in border control applications, for instance the US-visit program. Finally, under supervision or in controlled environments, it must be underlined that is very difficult to forge biometrics and impersonate a user, although it is much easier to forge documents.

ISO/IEC JTC1 SC37 Standing Document defines biometrics as: Automated recognition of individuals based on their behavioral and biological characteristics. A behavioral aspect of a biometric measures data pertaining to a personal trait, learned over time, or to a learned action. Biometrics with stronger behavioral aspects like keystroke, signature or voice can use acoustics, pressure, and speed whereas those with stronger biological aspects as fingerprint, iris, hand measure characteristics residing on or near the surface of the human body. The classification of biometric modalities is presented in following figure.

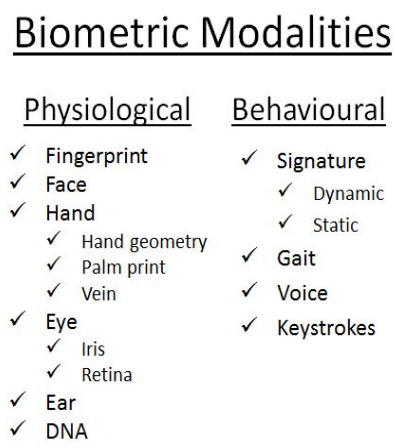


Figure 1: Biometric Modalities

A biometric scanning device takes a biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information which can be interpreted and verified. Since it is more difficult for a malicious hacker to gain access to a person's biometric data Biometrics can be used for both physical access to buildings and internal access to computers and systems:

- Face recognition
- Fingerprint scanning
- Hand scanning
- Iris scanning
- Keystroke recognition
- Retina scanning
- Signature recognition
- Voice recognition & DSV

A traditional biometric system is composed by four important modules:

1. The module **sensor** for capturing the trait in the form of raw biometric data.
2. The module **feature extraction** for processing the data to extract a feature set that is a compact representation of the trait. This set can be composed of biometric features that can be either ordered/grouped or not, depending on the biometric trait.
3. The module **matching** for employing a classifier to compare the extracted feature set with the templates stored in the database for generating matching scores.

The comparison is accomplished by the use of a distance function that can be Hamming distance, set difference, edit distance or Euclidean distance.

4. The module **decision** which uses the matching scores to either determine an identity or validate a claimed identity.

The accuracy of a biometric system can be measured by the following performance criteria:

• **False accept rate** or false match rate (FAR or FMR), meaning the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs being incorrectly accepted.

• **False reject rate** or false non-match rate (FRR or FNMR), meaning the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs being incorrectly rejected.

Biometric technology is used traditionally in the purpose of identification or authentication .

In the identification mode, the biometric system identifies a person from the entire enrolled users in the system by searching a match in a database, procedure called sometimes “one-to-many” matching. Another situation can be when a system can also be used in authentication or verification mode, where the biometric system authenticates the claimed identity of a person from their previously enrolled pattern. This can be called sometimes “one-to-one” matching.

When the matching is performed at the remote server, then the system is called as a remote biometric authentication. As having an alternative, biometrics can be used for local authentication - for example, controlling access to a private key on a smart card.

Applications based on biometric authentication can include workstation and network access, remote access to resources ,single sign-on, application logon, data protection, transaction security, and Web security. The e-commerce and e-government roles can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, health and social services, investing and other financial transactions, retail sales, and law enforcement are already benefiting from these technologies.

Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications [15].

The traditional cryptosystems are based on the standards and useed confirming that.

The encryption ciphers having the purpose of data confidentiality are presented in the following paragraphs in accordance with current standards of the encryption contained in ISO/IEC 18033-3-2010.

This standards specifies block ciphers. A block cipher is a symmetric encypherment system where the encryption algorithm operates on a block of plaintext to obtain a block of cypher text.

A plaintext is a well-defined length string of bits.

The following algorithms are specified:

- 64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT;
- 128-bit block ciphers: AES, Camellia, SEED.

ISO standards are reviewed every five years, so the last time this standard was reviewed in 2013.

Starting from 2000, when Rijndael [6] became the winner of the international contest of cryptographic algorithms, several kinds of comparisons between existing encryption ciphers have been made.

Comparisons have been attempted on the basis of the criteria hard or soft, as a function of time, the size of the encrypted texts, depending on the type of input date lot and more.

However a comparison only between AES, Camellia and SEED does not exist. This was the idea and the motivation that drove me to achieve this research presented below.

The following research was based on comparing the times required by the three algorithms in different situations depending on the size of the file entry. To this end 20 files were used for each algorithm, from sizes ranging between 10 kb to 50mb. Some programs for each situation were used and registered the times for the three encryption algorithms and for different keys, respectively 128 and 256 (where it exists, i.e. without SEED). At the same time, we take into account that it complies with an average over time, so each dimension has been tested by 5 runs and the average time was calculated. This way 900 tests were carried out for the key for 128-bit and 600 tests for the 256-bit. The computing systems used were two Asus laptops, both based on Intel microprocessors, Core i5 and Core i7.

III. EXPERIMENTAL RESULTS AND MATHEMATICAL CALCULUS

For the experimental research we used the OpenSSL library included in Ubuntu Linux 14.04 LTS. Linux operating system Ubuntu 14.04 LTS requires minimal maintenance. The computer systems used were two Asus laptops, both based on Intel microprocessors, core i5 and core i7. For testing we used files with the following dimensions: 10Kb, 20Kb, 30Kb, 40kb, 50kb, 100kb, 200kb, 300kb, 400Kb, 500Kb, 1Mb, 2Mb, 3Mb, 4Mb, 5Mb, 10Mb, 20Mb, 30Mb, 40Mb, 50M3. For each dimension mentioned above we have used 5 files, so the total number of files that were compared is 100 files. We have recorded the time required to encrypt files and also calculated and average time on the basis of the above mentioned.

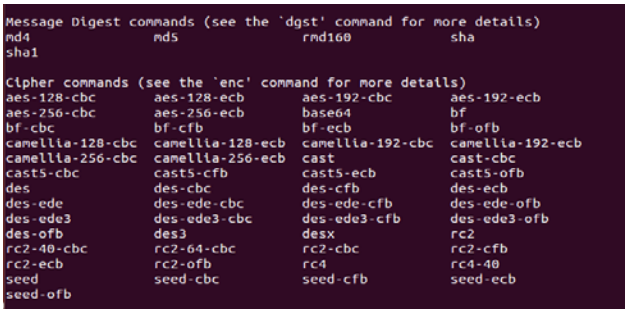
For encryption it was chose a 256-bit key AES and Camellia algorithms (SEED algorithm cannot operate with a 256-bit key) and the version with a 128-bit key for all three algorithms.

The 128-bit key used was: D3857ABEC68D4

The 256-bit key used was: E3C7671A5AD3839AAFBF79DB2596A.

Below you can see the command executed in Ubuntu 14.04 LTS a terminal to encrypt a file using the AES algorithm with a 128-bit key, open ssl library, followed by the command decryption under the same conditions.

For more details on using the open ssl library in UBUNTU 14.04 LTS the command man open ssl can be input from a terminal.



In this research it was presented a comparative analysis of the three encryption algorithms AES, Camellia and SEED.

An important goal is to know exactly which algorithm is more efficient depending on the size of the file encryption.

I't was presented the use of the Linear Feedback Shift Register for generating a pseudo-random sequence for increasing the difficulty of cryptanalysis [2].

A main part was the analysis of the Advanced Encryption Algorithm (AES) and for this a program in C++ was developed and used.

AES (Rijndael) with three possible key lengths (128 bit, 192 bit and 256 bit) provides a very high security and very fast software and hardware implementations.

Over time several kinds of comparisons have been made between algorithms. These comparisons focus on many evaluation criteria such as:

Security;

Hardware and software performances;

Resistance to power analysis and other implementation attacks;

Suitability in restricted space environments.

Another point of view is finding and using a methodology for evaluating the computational cost and the complexity of different block ciphers in order to be independent from the platform. This methodology is bridging the gap between the algorithms implementation and mathematical studies.

The main idea was to consider only the amount of the required operations, reducing all the transformations to byte wise-AND and byte wise-OR and shifts.

For each of the analyzed algorithms the implementation computational cost was calculated.

Software implementation of cryptographic algorithms using the same processor was another kind of analysis and another type of comparison.

The ISO Standard Block Ciphers were compared taking into account their ASIC Performance.

For this comparison the base idea was to research the efficiency of all the known ISO Standard Algorithms, function of the possible implementation for S-Box.

Another comparison for Block Ciphers was focused on the Hardware Performance. After a general hardware description for each of the algorithms compact and high-speed hardware architecture were proposed and evaluated [11].

All algorithms obtained similar performance in compact implementations. Also, it was proved that $GF(((2)^2)^2)^2$ inverter is smaller than $GF((2^4)^2)$ by 26%.

In this frame we research and obtain a complete analyze of using Shift registers in Cryptosystems for 4-th, 8-th , and 16-th degree Irreducible Polynomials was presented in Transaction on Computers [10].

Various features of files like: data density, data types, key size and data size have been analyzed using different symmetric key algorithms. The obtained results concluded that the date size and encryption time is proportional to each other.

At the same time encryption depends only upon the dimension of the file, not upon the data type or density.

We have analyzed the AES algorithm by creating an original program in C++.

We made a comparison between the three specified ISO/IEC 18033-3-2010, 128-bit block ciphers: AES, Camellia and SEED.

After research some practical aspects have been measured.

In the following rows two tables will be presented.

The first one will show a comparison of various Biometric Technologies Based on the Perception of the Authors: High, Medium and Low being denoted as H, M and L, Respectively [14].

Table 1. Comparison of Various Biometric Technologies

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

In the following table some information will be shown containing classification, privacy protection, practicality, sensitivity and security.

For the third column R and G significance is Release Key for R and Generation Key for G.

In the last four columns H, M, and L denoted high, medium and low.

Where the security results has not been provided it was denoted with U.

Table 2. Comparison of Various Biometrics-Based on Key Generation and Key Release Algorithms

Algorithm	Biometric (representation)	Classification	Privacy protection	Practicality	Sensitivity to invariance	Security
Soutar et al.	Fingerprint (image)	R	H	M	H	U
Davida et al.	Iris (IrisCode)	G	H	H	L	U
Monrose et al.	Keystroke, Voice	G	H	H	H	M
Linnartz and Tuyls	No evaluation	G	H	L	L	H
Juels and Sudan	No evaluation	G	H	H	L	H
Clancy et al.	Fingerprint (minutiae)	G	H	H	M	H

Based on the Shannon Theory of Communication [12] some aspects of developing Coding Theory were obtained by Berlekamp [5] and Van Lint [13].

The image for Fingerprint represents the object for the research obtained by Soutar et al [1].

For the other field of research focused on Iris, Davida et al. [3] gave some experimental results. Monroe et al. [7] developed a research in generating cryptographic keys by using voice.

Some other researchers focuses on developing secure smart card based on fingerprint authentication as Clancy [4].

Juels [9] developed a fuzzy commitment scheme and Linnartz and Tuyls [8] researches the possibility to prevent misuse of biometric templates.

In the next table the main Biometric Technologies will be presented.

It was completed in the first column the specification and in the second one the most important characteristics about acceptance, cost and others.

Table 3. Biometric Technologies

Face Recognition	Widely acceptable to users; low cost; no direct contact
Fingerprint	Mature technology; highly accurate; low cost; small size
Hand/Finger	Accurate and flexible
Iris	Highly accurate;
Keystroke Recognition	Low cost; uses existing hardware
Retina	Highly accurate
Signature Recognition	Widely acceptable
Voice Recognition	Usable over existing telephone system

IV. CONCLUSION

Identity of a person can be represented by using passwords and cards and our actual life prove that these are no longer suffice. Further, passwords and cards can be shared and thus cannot provide non-repudiation. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as facial patterns, fingerprints, eye retinas and irises, voice patterns, and hand measurements, used especially for authentication purposes. Biometrics, which uses biometric identifiers cannot be shared or misplaced so that automatic recognition of people based on their distinctive anatomical could become an essential component of effective person identification solutions.

A biometric system is a pattern-recognition system that recognizes a person by using a feature vector derived from a specific physiological or behavioral characteristic of the person. Depending on the application context, a biometric Authentication Process operates in one of two modes: identification or verification through Acquisition, Creation of Master characteristics, Storage of Master characteristics, Acquisition, Comparison and Decision. Acceptability is generated by software interpreting of the resulting date received capturing the salient human characteristic through the hardware.

Any system assuring reliable person recognition must necessarily involve a biometric component. Because of the unique person identification potential provided by biometrics, they will continue to provide useful value by identifying criminals, and eliminating fraud. The identification of new uses for biometric devices serve the potential for very low cost over the longer term. Biometrics is one of the important and more interesting pattern recognition applications with its associated unique business, legal, and political Challenges Biometric technology is an emerging technology and always considered realistic performance expectations and not fairly compared with existing alternatives, such passwords. Really, a successful biometric solution cannot be 100% accurate or secure. Each particular application can have a satisfactory performance justified through the additional investments needed for the biometric system. The designer can build the application context confirming to achieve the target performance levels.

In this work, we have proved the necessity for a widespread adoption of biometrics as being the best choice of automatic person identification.

REFERENCES

[1] Soutar C., Roberge D., Stojanov S., Gilroy R., and Vijaya B., Biometric encryption using image processing, Optical Security and counterfeit deterrence techniques II, 1998;

[2] Alfke P., Efficient Shift Registers, LFSR, Counters, and Long Pseudo-Random Sequence Generators, XAPP 052, July 7, 1996.

[3] Davida G., Frankel Y., and Matt B., On enabling secure applications through off-line biometric identification, IEEE Symp. Privacy and Security, 1998.

[4] Clancy T., Kiyavash N., and Lin D., Secure smartcard-based fingerprint authentication, Proc. ACM SIGMM Multimedia , Biometrics Methods and Applications Workshop, 2003.

[5] Berlekamp E. R., Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[6] Daemen J., Rijmen V., "*The Design of Rijndael: AES - The Advanced Encryption Standard"*, Springer-Verlag, 2002.

[7] Monroe F., Reiter M., Li Q., and Wetzel S., Using voice to generate cryptographic Keys, Speaker Recognition Workshop, 2001.

[8] Linnartz J., Tuyls P, New shielding functions to enhance privacy and prevent misuse of biometric templates, Proc. 4th Int. Conf. Audio-and Video Based Biometric Person Authentication, 2003.

[9] Juels A., and Wattenberg M., A fuzzy commitment sceme, Proc. 6th ACM Conf. Computer and Communication Security, 1999

[10] Mioc M. A., A complete analyze of using Shift Registers in Cryptosystems for Grade 4, 8 and 16 Irreductible Polynomials", WSEAS Transactions on Computers, Volume 7, Issue 10, ISSN: 1109-2750, October, 2008.

[11] Panda A. K., Rajput P., Shukla B., FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximum Length Feedback Polynomial Using VHDL, Rajkot, India, 2012.

[12] Shannon C.E., Mathematical Theory of Communication, 1948.

[13] Van Lint J.H., Introduction to Coding Theory, 2nd ed., Springer-Verlag, USA, 1992.

[14] Umut U., Sharath P., Salil P, Anil K.J., Biometric Cryptosystems: Issues and Challenges, Proceeding of the IEEE, vol.92, no.6, June 2004.

[15] Podio and Dunn, Digital Rights Management and Health Care applications, 2001.