Chapter

Digest: A Biometric Authentication Protocol in Wireless Sensor Network

Faezeh Sadat Babamir and Murvet Kirci

Abstract

Since the security of biometric information may be threatened by network attacks, presenting individual's information without a suitable protection is not suitable for authorization. In traditional cryptographic systems, security was done using individual's password(s) or driving some other data from primary information as secret key(s). However, encryption and decryption algorithms are slow and contain time-consuming operations for transferring data in network. Thus, it is better that we have no need to decrypt an encrypted trait of an enrolled person, and the system can encrypt the user trait with the user's passwords and then compare the results with the enrolled persons' encrypted data stored in database. In this chapter, by considering wireless sensor networks and authenticating server, we introduce a new concept called "digest" and deal with its efficiency in dealing with the security problem. A "digest" can be derived from any kind of information trait through which nobody can capture any information of primary biometric traits. We show that this concept leads to the increase of the accuracy and accessibility of a biometric system.

Keywords: biometric authentication, wireless sensor networks, system security, cryptography, digest

1. Introduction

A biometry of a person is a physical/logical property that is obtained from trait of the person. Since traits, details vary from person to person and no two people have the same trait, so the trait can be used as an ID in authentication/identification systems. Trait is a biological property of a person like fingerprint, retinal, iris, deoxyribonucleic acid (DNA), etc. The biometric authentication system collects traits of legitimate persons and stores them in database safely in order to use for identification of them in verification time, access time to data or place, etc. Moreover, implementing an authentication system through biometric data can create a secure guarded port for secure data or a place. This biometric security system is a lock and capture mechanism for access control [1]. In order to develop such a system, traits of legitimate persons should be scanned and stored in a safe database. When biometric security system is activated for authentication, it verifies and matches traits of persons with ones in database [1].

Wireless sensor networks (WSNs) are general networks that are employed in several applications, including military, medical. In all these cases, data security and energy usage are the determining factors in the performance of critical applications. Consequently, methods of protecting and transferring data to the base station are very important because the sensor nodes run on battery power and the energy available for sensors is limited [2].

In order to implement a flexible biometric security system, we need a favorite channel for transmitting information/data. This channel should be a safe and quick passage to transmit biological traits information/data. Since most of the time, accessing secure channel is costly or impossible, we would use a WSN channel for connecting capturing equipment such as scanner to DB. Obviously, this kind of network is not an enough safe passage for transferring highly secure information/data, because an enemy may capture secure data being transmitted. Therefore, we should code or encrypt them such that it may be incomprehensible for others and enemies are not able to abuse them. This process could be done by integrating with a biometric cryptography algorithms and WSNs [3].

Moreover, we use cryptographic algorithms for raw highly secure information to convert them to ciphertext. This task provides security as well as privacy.

Current authentication systems mostly are based on ID and password authentication system. Password is a combination of characters, numbers and letters that should be renewed in certain periods to prevent unauthorized people accesses. In order to provide an almost perfect secure system, a biometric security system can be implemented for authentication. But as mentioned above, the main problem is sending and receiving secure data/matching result through unsafe network. It means that network security should be considered as part of security performance for evaluation of security level of a biometric security system [3].

In this paper, we investigate a biometric security system proposed in [4] in WSNs. It saves a print of individual biometric traits through especial framework called "digest," which is output of a one-way function. This framework supplies perfect security without carrying out any encryption or decryption processes. Therefore, it would be a good selection for privacy preserving of users who wish to be authorized through a WSN. In order to make highly memory performance homomorphic property is utilized. This issue improves the algorithm energy consumption in WSN. Finally, Hamming distance measurement is used to compare stored data with newly created data to make decision of matched or mismatched in based node.

2. Related work

There are many studies that present power complexity efficiency methods in wireless sensor networks. These studies applied natural algorithms including genetic algorithm to find best method for transferring data [3–5].

The primary authentication mechanism is fingerprint whereas it is currently being pushed by the majority of smartphone/personal computer vendors. This solution is so simple due to the fact that our fingerprints could be obtained from everywhere that we were and touched before [6, 7]. Therefore, utilizing some individuals features are recommended to be used as a standalone authentication approach. Most of the smartphone vendors install an additional camera to obtain the fingerprint [8].

Key binding algorithm is used in [9, 10] for fingerprint matching system. Moreover, a cryptographic key will be bind with the user's fingerprint images at the time of enrolment.

Davida et al. [11, 12] proposed the iris based biometric for, authentication process. Moreover, binary representation of iris texture, called IrisCode [13] is considered. Also the Hamming distance compared the input and database template representations with a threshold to determine the matching result.

Monrose et al. [14] combined passwords with keystroke biometrics in secure way. Their technique was inspired by password "salting." Disadvantage of this method is that it only adds about 15 bits of entropy to the passwords. This leads marginally security. In [15, 16] they made some minor modifications to their primary work. They applied voice biometrics instead of keystroke. Tuyls et al. in [17, 18] supposed that all template are noise-free of a biometric identifier. Thus, they used them directly in to generate a secret named helper data W.

Juels and Wattenberg Davida et al.'s methods [11, 12] to tolerate variance in "fuzzy commitment" scheme [19]. This provides more strong security. Juels and Sudan [20] showed the security of the fuzzy vault scheme in an information-theoretic sense. Clancy et al. [21] extended Juels and Sudan [20] work. Moreover, they used "fingerprint vault" for multiple (typically five) fingerprints of users.

Michelin et al. [22] proposed the use of the smartphone's camera for facial and iris recognition by the decision-making using the cloud. Another work on biometric authentication for an Android device [23] showed an increased level of higher task efficiency achieved using various solution. In [24], authors studied the usability and practicality of biometric authentication in the workplace and concluded that the ease of technology utilization and its environmental context play a vital role while the integration and the adoption will always incur additional and unexpected resource costs.

The gesture-related user experience research conducted in [25–28] showed that security and user experience do not necessarily need to contradict each other. This work also promoted pleasure as the best way for fast technology adoption. In [26], authors addressed the usability of the ECG solution for authentication and concluded that the application of ECG is not yet suitable for dynamic real-life scenarios.

3. The protocol

Here, we explain the proposed biometric cryptosystem [4] based on Finite Composite order group as well as a figure that clears logical relationship between important parts of the system (**Figure 1**). The security degree of the system depends on a hard DLP [29].

For a high security level (with selection of very large factors), factoring N (if N = nm such that (n, m) are coprime numbers) is impossible. Disadvantage of this technique is that performing group operation for large composite groups is slow leading to complicated operations. This system is based on a special *generator* to resist many attacks making the system faster. Below, we explain steps of the proposed biometric cryptosystem.

3.1 KeyGen(π)

Let d be a security parameter of the system. Let m, p and q denote very large random prime numbers in which $n = pq$ and $N = nm \therefore n < m \ \& \ (n, m) = 1$. We define m and n as modulus for biometric trait. Also we know that $\varphi(N) = \varphi(mn) = \varphi(m)\varphi(n) = \alpha\beta$.

Let $X \equiv a \ mod \ m$ and $X \equiv b \ mod \ n$, $(m, n) = 1$, $(a, b) \geq 0$, $(\forall X < \alpha)$. According to the Chinese theorem [10, 11], we have:

$$X \equiv N_1 s_1 r_1 + N_2 s_2 r_2 \ (mod \ N) = m \, m_n^{-1} b + n \, n_m^{-1} a \ mod \ N \tag{1}$$

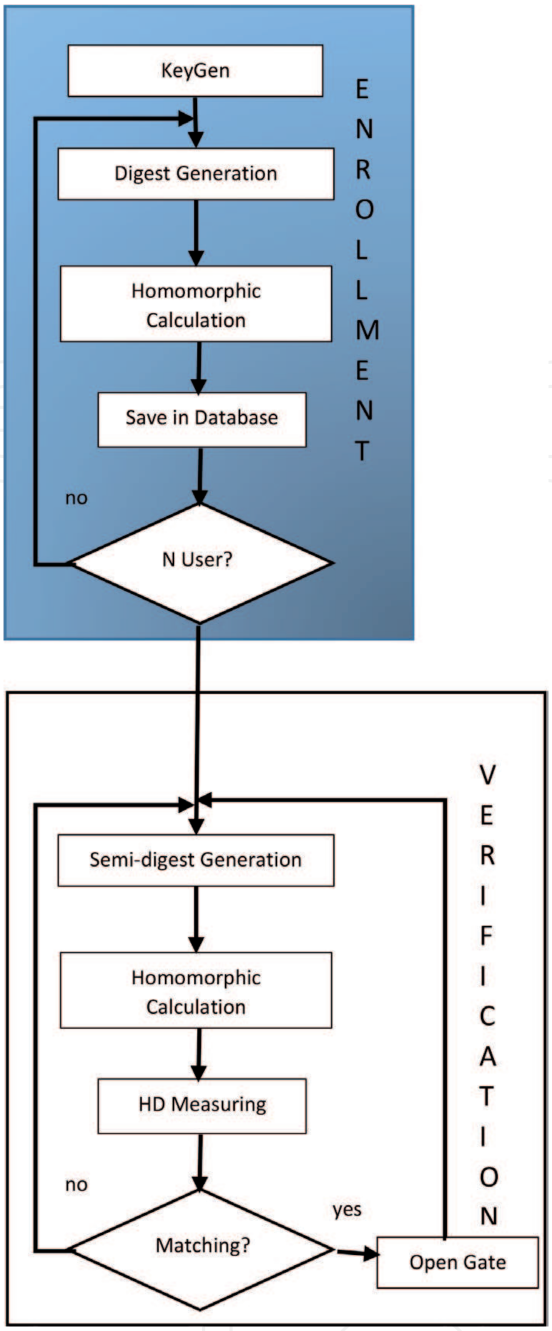

Figure 1.
The biometric authentication cryptosystem.

In Eq. (1) m_n^{-1} is the inverse of $(m \text{ mod} n)$ and n_m^{-1} is the inverse of $(n \text{ mod } m)$. Also $v = m m_n^{-1}, u = n n_m^{-1} \therefore (u, \alpha) = 1$.

We choose public system parameters as $< g, m, n, N, u, \alpha >$, and master secret key as $MSK = <\varphi(N) >$. Where G be a cyclic group with generator $g \in \mathbb{Z}_{\mathbb{N}}$ and $ord(g) = \alpha$. Also, β and so $\phi(N)$ should kept secret.

3.2 Enrollment (UK, SK, X)

In this phase, we measure biometric trait (X) to obtain value $\mathrm{R} = [X - bv]\ mod\ N$. Then system calculates k_{client} from Eq. (2), and saves this value to the memory.

$$D(X) = k_{client} = g^{R\beta}\ mod\ N \therefore \beta = \varphi(n) \qquad (2)$$

For every client and erases, all values except k_{client} of client, will kept in the memory of the system for verification process. If everyone access to k_{client}, she/he cannot obtain no information about X or R.

3.3 Verification $(\mathrm{UK}, \mathrm{X}')$

In authentication time, client calculates following equation:

$$h = Xu \; mod \; N \rightarrow D = g^{h+r\alpha} \; mod \; N \therefore r \in \mathbb{Z}^{*}_{\mathbb{N}}, \alpha = \varphi(m) \tag{3}$$

In Eq. (3), r is a random number. Client sends D to the system for verification process. System receives D and verifies:

$$\mathrm{D}^{\beta}_{\mathrm{client}} \bmod \mathrm{N} \xrightarrow{?} \mathrm{k}_{\mathrm{client}} \tag{4}$$

Correctness: we now describe that how verification performs efficiently. From Eq. (4), we have:

$$D^{\beta} = \left[g^{h+r\alpha} \; mod \; N\right]^{\beta} = \left(g^{h\beta} \; mod \; N\right)\left(g^{r\alpha\beta} \; mod \; N\right) \tag{5}$$

According to the Euler's totient function [10], the Eq. (5) equals to Eq. (6):

$$\rightarrow \left(g^{h\beta} \; mod \; N\right) \times (1) = g^{h\beta} \; mod \; N \xrightarrow{?} k_{client} \tag{6}$$

Homomorphic verification: the scheme turns out to be useful in homomorphic verification over an additive group, i.e., if $D(h)$ be randomized biometric digest $X \in \mathbb{Z}_N$, with respect to the public parameter N, we have Eq. (7):

$$D(h_1).D(h_2) = D[(h_1 + h_2) \; mod \; N] \therefore \forall h \in \mathbb{Z}_{\mathbb{N}} \tag{7}$$

HD measuring (M, D, M′, D′): the protocol check HD of parameter of Eq. (8), with all one in database along with their mask vectors. Note that:

$$HD\left(M, D, M', D'\right) = \frac{\left\|\left(D \oplus D'\right).M.M'\right\|}{\left\|M.M'\right\|} \tag{8}$$

Matching (HD, ι): Now the protocol compare obtained value to make final output according to Eq. (9)

$$\mathrm{result} = \begin{cases} \mathrm{matched} \; \mathrm{HD} \leq \tau \\ \mathrm{mismatched} \; \mathrm{o.w.} \end{cases} \tag{9}$$

The protocol includes two main phases: enrolment and verification. Every user should be enrolled through entering his/her biometric features using available instruments in the enrolment phase [30]. These instruments capture images and then process them to output vectors of *feature* and *mask* to cover errors as possible and send them to the enrollment algorithm [4, 31].

The protocol does not save original information in database. Instead, the protocol keeps the information in cache for just some seconds in order to process it using mathematical one-way functions and convert it to different data with different formats and natures. The final processed data *Digest*; Digests are values that nobody even system itself can identify the owner and the biometric property of the corresponding digest. Different digests of client will be fused with homomorphic operation. Additionally, he/she cannot misused available digests, because at authentication request time or online mode, system accept just semi-digest data as input that needs one more processing step to output digest [4].

After generating all of fused digests, all of primary information is safely erased from the cache memory and the digest is transmitted to the system database. The database is set of all original digests whose owners and biometric properties are unknown. Hereafter, if an individual wants to enter the system, the system will be able to identify him/her correctly as an authorized/unauthorized client [4].

After completing the enrollment phase and enrolling clients' digests, the system runs verification process, i.e., it enters the verification time of the protocol. An individual who request for authentication, enters his/her biometric information and the system captures it, process it to make fused semi-digest [4].

From now one, the protocol starts comparing algorithms. It firstly combines semi-digest with the secret parameter of the system to generate the corresponding digest. This digest will be compared with available digests in the database. This matching will be carried out using computation of the Hamming Distance measure of four parameters: (1) the stored digest, (2) its mask vector, (3) the new digest, and (4) its mask vector. If the obtained HD is fewer than value of threshold τ, the client's identification has been matched [4].

4. The protocol analysis in WSNs

In this section, we compare the scheme [4] with those of [9–12, 14, 17, 20, 21]. Moreover, we review properties of the protocol that were performed on a single core of an Intel®, Pentium® D, 3:2Ghz processor, using MATLAB R2016a. Also we used Miracle library in binary fields [32] for some mathematical operations.

In this case, we installed the Java Genetic Algorithm Package (JPAC) to test the algorithm in a manner consistent with prior studies. Next, we utilized OMNET++ to trace the movement of the nodes in a virtual environment.

Algorithm	Biometric representation	Classification	Privacy preservation	Practicality	Sensitivity to invariance	Security	Efficiency in WSNs
Murvet et al. [4]	Fingerprint, iris	G	H	H	L	H	L
Soutar et al. [9, 10]	Fingerprint	R	H	M	H	U	M
Davida et al. [11, 12]	Iris	G	H	H	L	U	L
Monrose et al. [14]	Keystroke, voice	G	H	H	H	M	M
Linnartz et al. [17]	No evaluation	G	H	L	L	H	L
Juels and Sudan [20]	No evaluation	G	H	H	L	H	H
Clancy et al. [21]	Fingerprint	G	H	H	M	H	H

Table 1.
Comparison between various algorithms.

In **Table 1**, a comparison between various algorithms in WSNs: the proposed scheme in [4], Soutar et al. [9, 10], Davida et al. [11, 12], Monrose et al. [14], Linnartz and Tuyls [17], Juels and Sudan [20], and Clancy et al. [21] are given. The third column in **Table 1** indicates the key release (R) or key generation (G) classification. Column "Practicality" deals with the complexity of the algorithm. Last column shows the efficiency of algorithms in WSNs.

The protocol operates based on new concept *digest* [4] that leads to reduce time complexity of the proposal compared to schemes that already used encryption and decryption process.

This concept also improved efficiency of identification operation in cost and time as well as it is safe enough to customize for any application.

5. Conclusion

Wireless sensor networks are flexible and useful networks for securing critical data through biometric authentications. However, they are powered by nodes equipped by the limited capacity batteries. On the other hand, biometric authentication brings greater convenience to users than other authentication systems. This method can perfectly protect legitimated users and data against internal malicious and external frauds. Moreover, this measures and analyzes user's unique information for automatically recognizing user's identification. The first five most common traits are fingerprint, hand, eye/Iris, face and voice that would be transmitted through WSN. In this study, we utilized Iris and fingerprint to make a strong biometric authentication system in WSN. The scheme proposed in [4] was the more efficient in terms of applicable efficiency in WSN in comparison with similar studies. As a future work, the system will be able to operate in any networks by applying property of "Boolean identification." Further, by studying other difficult problems, we will improve this study to gain linear time efficiency. These new properties help networks to transmit data securely and efficiently in any sensitive network.

Author details

Faezeh Sadat Babamir* and Murvet Kirci
Istanbul Technical University, Maslak, Turkey

*Address all correspondence to: babamir@itu.edu.tr

References

[1] Jain AK, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security. July 2006;**1**(2):125-143

[2] Norouzi A, Babmir FS, Zaim AH. A novel efficient routing protocol in wireless sensor network. Wireless Sensor Network Journal. October 2011;**3**(10):341-350

[3] Reid P. Biometrics for Network Security. Boston, USA: Pearson Education Inc.; 2004. ISBN: 0131015494

[4] Kirci M, Babamir FS. A digest based method for efficiency improvement of security in biometrical cryptography authentication. In: IEEE International Symposium on Computer Science and Software Engineering; 2017

[5] Norouzi A, Babamir FS, Zaim AH. An interactive genetic algorithm for mobile sensor networks. Studies in Informatics and Control. 2013;**22**(2)

[6] Jain A, Bolle R, Pankanti S. Biometrics: Personal Identification in Networked Society. Vol. 479. Berlin, Germany: Springer; 2006

[7] Maltoni D, Maio D, Jain A, Prabhakar S. Handbook of Fingerprint Recognition. 2nd ed. Berlin, Germany: Springer; 2009

[8] Le C. A Survey of Biometric Security Systems. A Report. USA: Washington University in St. Louis; 2018

[9] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption using image processing. In: Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques II; Vol. 3314; 1998. pp. 178-188

[10] Cavoukian A, Stoianov A. Biometric encryption. In: Nichols RK, editor. ICSA Guide to Cryptography. New York: McGraw-Hill; 1999

[11] Davida GI, Frankel Y, Matt BJ. On enabling secure applications through off-line biometric identification. In: Proceedings of the 1998 IEEE Symposium on Privacy and Security; 1998. pp. 148-157

[12] Davida GI, Frankel Y, Matt BJ, Peralta R. On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Proceedings of the Workshop Coding and Cryptography (WCC'99); 1999. pp. 129-138

[13] Ang R, Safavi-Naini R, McAven L. Cancellable key based fringerprint templates. In: Australasian Conference on Information Security and Privacy; 2005. pp. 242-252

[14] Monrose F, Reiter MK, Wetzel S. Password hardening based on keystroke dynamics. In: Proceedings of the 6th ACM Conference on Computer and Communications Security; 1999. pp. 73-82

[15] Monrose F, Reiter MK, Li Q, Wetzel S. Using voice to generate cryptographic keys. In: Proceedings of 2001: A Speaker Odyssey, Speaker Recognition Workshop; 2001. pp. 237-242

[16] Monrose F, Reiter MK, Li Q, Lopresti DP, Shih C. Toward speech-generated cryptographic keys on resource constrained devices. In: Proceedings of the 11th USENIX Security Symposium; 2002. pp. 283-296

[17] Linnartz J-P, Tuyls P. New shielding functions to enhance privacy and prevent misuse of biometric templates. In: Proceedings of the 4th International Conference on Audio- and Video-Based Biometric Person Authentication; 2003. pp. 393-402

[18] Verbitskiy E, Tuyls P, Denteneer D, Linnartz JP. Reliable biometric authentication with privacy protection. Presented at the SPIE Biometric Technology for Human Identification Conference, Orlando; 2003

[19] Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proceedings of the Sixth ACM Conference on Computer and Communication Security; November 1999

[20] Juels A, Sudan M. A fuzzy vault scheme. In: Proceedings of the IEEE International Symposium on Information Theory; Lausanne, Switzerland; 2002. p. 408

[21] Clancy TC, Kiyavash N, Lin DJ. Secure smartcard-based fingerprint authentication. In: Proceedings of the ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop; 2003. pp. 45-52

[22] Michelin RA, Zorzo AF, Campos MB, Neu CV, Orozco AM. Smartphone as a biometric service for web authentication. In: Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST); Barcelona, Spain; 5-7 December 2016. pp. 405-408

[23] Conti V, Collotta M, Pau G, Vitabile S. Usability analysis of a novel biometric authentication approach for android-based Mobile devices. Journal of Telecommunications and Information Technology. 2014;**4**:34-43

[24] Maple C, Norrington P. The usability and practicality of biometric authentication in the workplace. In: Proceedings of the First International Conference on Availability, Reliability and Security; Vienna, Austria; 2006. pp. 1-7

[25] Aumi MTI, Kratz S. AirAuth: Evaluating in-air hand gestures for authentication. In: Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services; Toronto, ON, Canada; 23-26 September 2014. New York, NY, USA: ACM; 2014. pp. 309-318

[26] Da Silva HP, Fred A, Lourenço A, Jain AK. Finger ECG signal for user authentication: Usability and performance. In: Proceedings of the 6th International Conference on Biometrics: Theory, Applications and Systems; Arlington, VA, USA; 29 September–2 October 2013. pp. 1-8

[27] Katz J, Lindell Y. Introduction to Modern Cryptography. Chapman and Hall/CRC; 2014

[28] Trapper W, Washington LC. Introdunction to Cryptography with Coding Theory. Upper Saddle River, NJ, USA: Prentice-Hall, Inc; 2005

[29] Babamir FS, Bayat F. Linearly Time Efficiency in Unattended Wireless Sensor Networks. Rijeka, Croatia: InTechOpen; 2012. pp. 213-226

[30] Daugman J. The importance of being random: Statistical principles of iris recognition. Pattern Recognition. 2003;**36**(2):279-291

[31] Babamir FS, Norouzi A. Achieving key privacy and invisibility for unattended wireless sensor networks. The Computer Journal. Oxford University Press; 2014;**57**(4):624-635

[32] Maltoni D, Maio D, Jain A, Prabhakar S. Hanbook of Fingerprint Recognition. 2nd. New York city, USA: Springer; 2009. https://www.miracl.com/