Upgrading Existing Biometric Security Systems by Implementing the Concept of Cancelable Biometrics

Miroslav Bača
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
miroslav.baca@foi.hr

Marko Antonč
Invita d.o.o.
E. Kotromanč 7, 23000 Zadar, Croatia
marko.antonic@gmail.com

Magusic Franjo
Visoka policijska skola Zagreb

Abstract. *Today's biometric security systems have a number of problems that emerge from the fact that the biometric data of a person is stored in the system. The problems arise when that data is compromised. Standard password based security systems have the ability to cancel the compromised password and reissue a new one. The biometrics cannot be canceled or changed which can be their advantage and a disadvantage in this particular situation. The concept of cancelable biometrics can upgrade the biometric security system so that it gains the advantages of the password based security system, by not losing the inherent superiority.*[1]

Keywords. Cancelable biometrics, revocable biometrics

1 Introduction

Standard biometric system functions consist of two phases. The first phase is *enrolment phase,* in which the user's biometric template is acquired. The second phase is *authentication phase*. In the authentication phase, biometric sample is taken from the user and compared to the biometric template stored in the database. If they match, positive authentication is achieved.

The fact that the biometric data of every user in that system is stored in a database opens a few potential problems.

- *Identity theft* – the attacker steals the biometric data from the database and using that data constructs an artifact which can be used to impersonate the original user. The artifact can be an artificial finger, artificial eye, face mask, photography, or something else depending on the type of the biometrics in database.
- *Irrevocability* – the nature of biometric sample is such that they are permanent. Consequently a user shouldn't be able to change the template acquired. For instance, a fingerprint of right index finger, once given, cannot be changed. The fact that biometric templates, once issued, cannot be reissued, changed or revoked, in comparison to passwords, is considered to be a major concern.
- *Exposure of personal information* – it has been proven that fingerprints, besides information about *minutiae* which is used in authentication phase, also relieves some information about genetic origin of a person. Retina scan can reveal existence of some diseases like diabetes or stroke [1]. All these information is considered personal and as such shouldn't be revealed to anyone without our consent. More than that, some critics of biometrics systems claim that every biometric sample is personal information by itself, and as such, shouldn't be used at all [8]. And, since forcing the user to reveal his personal information is illegal, the use of biometrics should be forbidden.
- *Scope of use* – biometric sample should be used only for the purpose it was given for. Any situation in which that scope is overridden is considered an invasion of privacy. The situation in which the

[1] 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.

police decides to use the database of biometric templates of a bank, which contains biometric templates of users for the purpose of authentication prior to giving access to vaults, and uses it to identify a criminal, should be strictly forbidden.

The increasing demand for more secure and convenient security systems generates an increase in number of biometric systems installed. Existence of many biometric systems yields the need for the central biometric template storage. Motivation for this central storage comes from two different angles. The first is the fact that the enrollment phase is relatively costly [3]. Since every user has to go through that process, and the number of systems is large, the process will be repeated many number of times. Repeating one process many times is inefficient and inconvenient for the user. The central template storage place is a good solution to avoid the extra cost and inconveniences. The second motivation is standardization. Central biometric template storage would force all the members of a group of services that use biometric authentication to use the same, standardized methods. The whole process of authentication would have to be standardized, starting from sensors over algorithms to security policies. Standards would solve the compatibility problem over different services within the group and enable a possibility for adding a new service to the group. This kind of centralized storage opens many concerns for the user. Who has the right of usage? Who has the access? How can the user limit someone's access? How can the user trust all the member services in the group?

There exist a number of solutions all of which relying on the hiding of biometric template in the storage. One is a classical approach to protecting sensitive data in IT industry – data encryption. Clearly encryption is not the ultimate solution, since the template has to be encrypted prior to matching with the new sample, and is that moment exposed in its original form. The second, more secure method is cancelable biometrics [2]. In this paper we will explore cancelable biometrics in more detail.

2 Cancelable biometrics

As long as the biometric template exists within the system, it is exposed to a potential attacker. But how to create a biometric security system that doesn't have stored biometric templates. Consider the case of an encrypted database of biometric templates. If we assume that the encryption is strong enough that brute force methods are not taken into account, then the templates are most exposed when they are decrypted. As a reminder, the template needs to be decrypted before it can be matched to a new sample. But if the template could stay encrypted it would be safe.

Cancelable biometrics is a concept in which the biometric templates are transformed into a different form. But, in contrast to encrypted templates, they do not need to be transformed back into their original form before they can be matched to new samples for authentication purposes. In fact, for the transformation function we choose the one which is noninvertible, so that the template cannot be transformed back into its original form even if we want it to. The matching is performed by transforming the new acquired sample with the same transformation, and then making the comparison in transformed space.

This concept ensures that the original biometric template doesn't exist in the system. As such, it is not in danger of being exposed. The privacy issue is this way completely nonexistent. If an attacker is able to get to a transformed template it will be completely useless to him. He cannot use it to construct an artifact which could enable him to impersonate user. Even more, the template couldn't be used for identification purpose, like for instance the police using it to find a criminal. Existence of transformation function allows simple control over which services have access and which don't. The authorized services will have the knowledge of the transformation function, and the other will not.

But this concept is not created only to address the privacy issues. The fact that the stored biometric templates are created by using a transformation function on the original biometric templates enables creation of new templates by using a different transformation function on the original biometric templates of the user. If one can generate a new biometric template, the old one can be canceled. Biometric security systems which implement the concept of cancelable biometrics can enjoy all the benefits we were used to in classic password based security systems (revocability and ability to reissue) but with preserving the benefits of biometric systems. Biometric templates are bind to the user so that they cannot be given to someone else.

They cannot be stolen or forgiven. And they have a greater resilience to brute force attack since they have a greater information size.

2.1 Usage scenario

Classic scenario of using biometric security systems which implement cancelable biometrics is very similar to the usage of classical biometric systems. First, a biometric sample is taken from the user during the enrollment phase. That sample is transformed by a chosen transformation function and stored as a template in a database. Afterwards in authentication phase after a sample is taken it is transformed by the same transformation function. The transformed sample is then matched to the template. If the template is stolen, the template is canceled and a new one is enrolled, only by changing the transformation function used. The transformation function by itself can be stored on a SmartCard or on the server along with the templates. It can be kept secret or publicly available, depending on the system implementation. If the function is noninvertible it can be kept together with the templates, and doesn't need a higher degree of protection.

2.2 Transformation on the signal level

The transformation of samples can be performed right after the sensor, on the signal level. The data it is performed on can be a picture of the face, fingerprint, picture of the iris or another kind of biometric sample. An example of such transformation is grid morphing. Grid morphing changes the picture, for instance a picture of a face. First a grid is positioned on a face so that it is aligned with face features like eyes, nose and chin. Then the grid is morphed so that the face is morphed with it. The result is another face that cannot be linked to original face. More information on grid morphing can be found in [10] and [11]. Even simpler example is the perturbation of blocks on an image. A fingerprint image can be divided into blocks and then the blocks positions are scrambled. Resulting image doesn't represent an actual fingerprint anymore, but an algorithm for finding minutiae will still have excellent results.

These kinds of transformations change the original biometric data in a way that existing algorithms for feature extraction still function on them after the transformation. Actually it is very important that they do not diminish the power of existing algorithms. The result of signal level transformations is actually another biometric data but not linkable to an actual person. The rest of the biometric security system is actually never even aware of the transformation of the signal.

One of the prerequisites for this kind of biometric system to function is that the applied transformation can be used to repeatedly transform the signal during the authentication phase in the same way. The problem of repeatability arises. The original biometric data is usually represented by a picture, but it could be any other human feature like scent or sound. No matter what kind of biometrics is used, in order to repeatedly apply the transformation in the same way, the signal has to be normalized. Some features of the biometrics have to be found prior to transformation. For instance, position of the face on picture, or position and angle of the iris, need to be found and the picture has to be normalized in a way that the found element is centered and in equal rotation. Only after that kind of preprocessing the transformation can be applied. The grid morphing example mentioned above has a grid that has to be aligned with the features of the face. Only after the eyes, nose, chin and other relevant features are found, the grid can be positioned, and the transformation can be applied. If the grid is not aligned the same way every time a transformation is applied, the resulting image will not be comparable to the stored biometric template of the user, and the authentication will fail. This process can be very difficult and sometimes impossible.

2.3 Transformation on the feature level

Besides transformation on the signal level, transformation can be applied on the feature level. The feature level of the biometric sample is represented by a list of features describing the biometric sample. It is usually represented by a list of numbers, like coordinates, angles or sizes. These numbers can represent fingerprint minutiae or sizes of fingers and palm in hand geometry biometrics. Transformation on feature level doesn't need the normalization which is crucial for transformations on signal level, since the sample is already processed and all the features are extracted into a normalized form.

Some feature level transformations change the biometric template so that the existing algorithms for matching still function on them without any need for adapting. One example of such function would be an

transformation of features that simply changes their position in coordinate space. But some change data into a form completely different from any known biometric data, like hash functions [7]. Such data cannot be matched using the same algorithms but require new, for that purpose created algorithms.

An example of feature level transformation is applying a high order polynomial function on every minutia in biometric template. An example of such function could be written as shown in eq. 1.

$$F(x) = \prod_{n=0}^{N}(x - \alpha_n) \quad (1)$$

Equation eq. 1 shows a polynomial function in factored form. The symbol N represents the order of a polynomial. If N is high, we consider this function to be a high order polynomial function. The function has multiple zeros, and as such cannot be inversed to simply obtain the origin of data. We could use it to irreversibly transform the fingerprint minutiae. If we represent the minutiae by a point set shown in eq. 2.

$$S = \{(x_i, y_i, \theta_i) | i = 1, \dots, M\} \quad (2)$$

Then we can construct three different polynomial functions F, G and H. First we define each polynomial function by defining its order, represented by the symbol N in eq. 1. After that we choose N different constants for α_n in eq. 1, for every function. Then we can use the function F on every x_i from eq. 2 to transform it to x_i' in eq. 3. We use the function G on y_i and H on z_i respectively.

$$S' = \{(x_i', y_i', \theta_i') | i = 1, \dots, M\} \quad (3)$$

By applying this function we have transformed the original minutiae set S into a new set S' which is different from the original. If the attacker had the new set S' and all three used transformation functions F, G and H, he would still be unable to retrieve the original set S.

Another example of a transformation function would be a series of perturbations of feature points. The same perturbations need to be repeatable on every new sample for that user, or otherwise authentication could never be performed, because comparison couldn't be done.

One of the main goals of cancelable biometrics is ensuring the biometric data of the person so that it can never be compromised. A transformation function can be similar to the previously mentioned perturbation based function, but with the addition of converting some features to zero or any other randomly chosen number [6]. That way, even if the attacker recreates the original template by inverting the perturbations on the transformed template, he wouldn't get the user's true identity because some of the features were irreversibly changed.

2.4 Transformation function

The function that is used during the transformation phase has to have certain characteristics.

Since we want to have the option of canceling and reissuing the template, we don't want a limited number of transformation functions which could be applied, because that would limit the possible number of cancel-reissue actions. We seek for a family of functions which has unlimited number of variations.

If we store the transformation function in the same place where we store the biometric templates, then it can be stolen along with the template. It is necessary that an attacker having the template and the transformation function that created it cannot get to the original template. The only way to ensure that is for a function to be noninvertible, or have large enough number of inverts that would discourage a brute force attack. If the function is not noninvertible, it should be carefully hidden form the attacker. One way to hide it would be to place it on a SmartCard and not in a shared storage.

Transformation function can enlarge the template size in bytes. Which is good because the time needed for a brute force attack on a security system (trying all possible combinations until we hit the one that will allow acces) increases exponentially by the size of the template size.

Transformed biometric templates should not diminish the uniqueness of a biometric data [9].

- Two different transformation functions applied on a same sample must differ (return false if compared).
- Result of a transformation T1 applied on a sample S1 should never be the same as

a result of a transformation T2 applied on a sample S2.

- Two different samples transformed by the same transformation function must differ.

These three preconditions need to be fulfilled in order to preserve uniqueness. Because biometric data of a person are usually quite similar from one person to the other, the standard matching function, which measures the distance between samples, needs to be very sensitive. The fact that we are no longer comparing original biometric samples which are determined by a person's biometric, enables us, by using adequate transformation functions, to ensure even higher uniqueness by making the difference between samples greater. By increasing the distance between biometric samples we can achieve lower FAR (false accept rate) without increasing FRR (false reject rate) [5].

We can conclude that the transformation function actually represents the essence of the concept of cancelable biometrics. As such it must ensure that it does not diminish the positive characteristics of biometric security systems. By choosing the right type of function we can even enhance the system by producing higher uniqueness.

3 Conclusion

The presented concept of cancelable biometric templates is a good solution to most of the perceived problems of today's biometric security solutions. Ensuring the original user's biometric data is never stored in the system not only addresses privacy issues, but also ensures that user's identity is never exposed, and as such is not in danger. The ability to cancel and reissue a biometric template is a giant step towards increasing the usability of biometric security systems since many critics are using that disability, very often used in classic, password based security systems, as the main obstacle in numerous arguments. Because of the nature of data being transformed it is probably easier to apply the transformation on the feature level. Choosing the appropriate transformation function is the hardest task in implementation of cancelable biometrics. The transformation function can ensure greater uniqueness among samples. A large family of functions must be chosen so that it is not limited in number of variations. It must be noninvertible. It should increase the template size. Finally, every system implementing cancelable biometrics should be carefully planned and tested to ensure that all of the mentioned goals are achieved.

4 Future research

In order for cancelable biometrics to achieve its full potential, it is necessary to choose the appropriate transformation function. More work should be done on finding the function that would maximize all the potential described benefits. The function should be tested thoroughly to ensure that it does not diminish uniqueness of the enrolled templates. Also the irreversibility of the function should be carefully analyzed.

Also the matching algorithm should be constructed if the transformed templates differ in nature from the original templates. The matching algorithm should be capable of maximizing the features of the new template.

The transform function should be embedded in the biometric sensor if possible, or placed very close to it, because transport of original sample should be very limited, and if in any way possible avoided. The needed biometric system architecture scheme changes should be explored, selected and tested.

References

[1] Pim Tuyls, Jasper Goseling: Capacity and Examples of Template-Protecting Biometric Authentication Systems, ECCV Workshop BioAW, Springer (2004).

[2] Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, vol. 40, pp. 614-634, (2001).

[3] Michael Braithwaite, Ulf Cahn von Seelen, James Cambier, John Daugman, Randy Glass, Russ Moore, Ian Scott: Application-Specific Biometric Templates, Auto ID (2002).

[4] Schneier, B. Secrets & Lies : Digital Security in a Networked World, New York, John Wiley & Sons, pp 141-145, (2000).

[5] Ying-Han Pang, Andrew Teoh Beng Jin, David Ngo Chek Ling: Palmprint based Cancelable Biometric Authentication System, International Journal of Signal Processing Volume 1 Number 2 (2004).

[6] Kar-Ann Toh, Chulhan Lee, Jeung-Yoon Choi and Jaihie Kim : Performance Based Revocable Biometrics, Biometrics Engineering Research Center, School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea, (2007).

[7] Sergey Tulyakov, Faisal Farooq and Venu Govindaraju: Symmetric Hash Functions for Fingerprint Minutiae, Springer (2005)

[8] Terrance E. Boult, Robert Woodworth: Privacy and Security Enhancements in Biometrics, Advances in Biometrics Sensors, Algorithms and Systems, Springer (2007).

[9] Andy Adler: Biometric System Security, Handbook of Biometrics, Springer (2007)

[10] G. Wolberg : "Image Morphing: A Survey", The Visual Computer, 14, pp. 360–372 (1998).

[11] T. Beier and S. Neely: "Feature-Based Image Metamorphosis", Proceedings of SIGGRAPH, ACM, New York, pp. 35–42, (1992).