Technical report, May 2007

Automatic Template Update Strategies for Biometrics

Tobias Scheidat, Andrey Makrushin and Claus Vielhauer

Otto-von-Guericke University of Magdeburg
Advanced Multimedia and Security Lab
Magdeburg, Germany

ABSTRACT

Some disadvantages of biometric systems are caused by intra-class variability that describes the fuzziness of biometric data given from a single person for one biometric characteristic. Reasons for example can be found in natural behavioral variability, poorly acquired biometric reference data, changing acquisition environments (e.g. alternating sensors) and/or in aging effects of the bearer of biometric information such wrinkles or injuries. The automatic exchange of biometric reference data sample in reference storage with another quality proofed biometric sample of particular person could greatly improve authentication performance of biometric systems. In this paper strategies are proposed to replace biometric reference samples adopting well known cache replacement strategies.

Keywords: authentication, biometrics, dynamic template, biometric references

1. INTRODUCTION

Nowadays the determination of the authenticity of persons and information is a recent topic of IT security. There are three main methods for user authentication: secret knowledge, personal possession and biometrics. Secret knowledge uses information for authentication purposes which is only known by the authentic person (i.e. password or personal identification number). For personal possession based authentication the user has to present a special token, e.g. key or smart card. Biometric systems use a physical (e.g. fingerprint, iris) or behavioral (e.g. handwriting, speech) characteristic of the person. While authentication objects of the traditional methods secret knowledge and personal possession can be lost, stolen or handed over the authentication object of biometric methods are linked with the body or behavior of the user directly and thus considered as more reliable for user authentication.

Basically, there are no identical biometric data sets based on one biometric characteristics given from the same person because of changes of the biometric trait itself (e.g. aging of bearer) and of the environment such changing sensor hardware. This drawback is described as intra-class variability by Ross and Jain in [2]. They also identify the inter-class similarity as a well known problem of biometrics which is the similarity of the biometric representations of the same characteristic of different people.

The problems mentioned above can be reason of non satisfactory recognition results during authentication. There are a lot of strategies to improve the authentication performance of biometric systems. Several approaches to improve the authentication performance of fingerprint recognition are proposed by Jain et al. in [1]. The authors show that an improvement can be achieved by withdrawing fingerprint images having a low quality or habituating users. An additional idea suggests the combination of more than one finger or more than one instances of the same finger. The fusion of biometric modalities, algorithms and instances based on one modality or sensor data is a recent topic of biometric research and tries to reach a better performance with regard to authentication than using the single components involved (see [2]).

For example, the fusion of four biometric handwriting algorithms is presented by Scheidat et al. in [3]. Using this so called multi-algorithmic fusion a relative improvement of the authentication performance of 12% was reached in comparison to the best single algorithm involved, based on equal error rate (EER, see section 2.2) as performance measure. Another method to improve the authentication performance is the automatic parameter optimization using genetic algorithms, which are based on fundamental concepts of natural evaluation processes such crossover or mutation to calculate a better generation of parameters based on an initial generation and a fitness function. In [4] such a genetic optimizer for biometric purposes is presented that works independently from the biometric system used. Based on a fingerprint recognition system, the authors report an improvement of the authentication performance of approximately 38% in the best case using this genetic optimizer.

A new idea for compensation of the described drawbacks of biometric systems is presented in this article. The replacement of insufficient elements of the references of a biometric system is presented based on cache replacement strategies. Cache or page replacement is a general problem in computer science and occurs in quite different fields. For instance most computers have one or more memory caches to speed up data access. Memory cache consists of last used memory blocks. When the cache is full, some block has to be chosen for removal. Second examples are Web servers, which can keep a certain number of heavily used Web pages in its memory cache. However, when the memory cache is full and a new page is referenced, a decision has to be made which Web page to evict [5]. In case of biometric systems the reference storage is considered as memory cache and reference vectors as blocks which should be always actual for user authentication.

The article is structured as follows: The next section gives a motivation of automatic template update. The basic strategies of cache replacement and the adaptation of cache replacement strategies for the replacement of single elements of biometric references are described in the third section. The last section gives a short conclusion of this paper and an outlook of upcoming work based on the ideas presented in this article.

2. AUTOMATIC TEMPLATE UPDATE

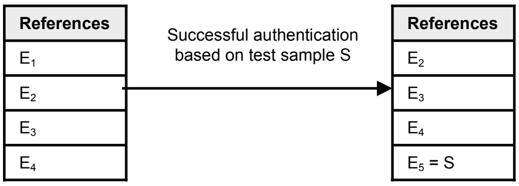
The biometric authentication performance in sense of error rates, which can be measured during authentication process, depends on a couple of system parameters: Biometric modality, quality of a sensor, feature extraction algorithm, presentation of extracted features, quality and quantity of reference vectors produced on enrollment phase, classification algorithm or system threshold are for example parameters which strongly influence the performance. On the assumption, that only the software part of an authentication system can be tuned and extracted features are fixed, it can be asserted that form and size of clusters, which are built from templates for each person, are parameters which most strongly influence classification process and thus system error rates. All classification algorithms do, is find out decision boundaries which better separate different clusters (persons). Based on this fact, it can be said that the performance depends rather on quality and quantity of biometric templates than on the classification algorithm. One problem such as mentioned earlier can be an aging of templates or users which can result in high intra-template variability. The most common technique used nowadays to solve this problem is periodic update of references, e.g. by reenrollment. Therefore the required biometric modalities of the persons will be acquired and registered again. The time interval in which this procedure should be repeated depends on different factors, such biometric modality, purpose of authentication or each person’s individual circumstances. For example the validity of biometric passports for travel abroad in most European countries is ten years for adults and five years for children. Such approach greatly reduces comfort of using the biometric system, because every registered person should be next to the system to present his or her changed biometric characteristic again, when the system works in enrollment mode. The next big problem of such approach is constant decreasing of authentication rate with aging of templates. Biometric systems authenticate properly only some days after registration of persons. The method proposed in this paper can be used to update the biometric reference data automatically in an easy way. The aim is to hold up-to-date reference data in biometric database for each registered person with a minimum of his or her interaction and completely avoid reenrollment process. To reach it, after every successful authentication the authenticated test sample should be included into the reference data. This sample is an anyway more up-to-date representation of biometric modality than every of template samples. So if it is sufficiently sure, that the current test sample is generated from the right legal person, it should be inserted into the reference storage. However, because the capacity of reference storage is limited, it can not contain all or lot of biometric references of each person. Therefore some of older or unnecessary template samples should be replaced by the authenticated test sample.

3. ADAPTATION OF CACHE REPLACEMENT METHODS

The aim is, to find out which reference data of the present person should be replaced by the current authentication sample. To answer this question, in this article the biometric references of each individual person in reference storage is considered as a cache - a temporary storage area where frequently accessed data can be stored for rapid access. So the idea is to use cache replacement strategies for replacement of biometric reference vectors in order to keep the references up-to-date. Such a strategy can be first in first out (FIFO), least frequently used (LFU), least recently used (LRU) or any other [6].

3.1 First in first out (FIFO)

The first in first out algorithm replaces the oldest template sample. It is one of the most simple strategies that can be used for replacement of biometric references. As shown in Figure 2 the reference data of each registered person can be seen as a queue of i slots (in this case i=4). After a successful authentication the oldest reference element (E_1), which was inserted first in the queue, is dropped and the authentication sample is pushed on the end of the queue as forth reference (E_5=S). Appling this technique we get only newest references of biometric modality in database. However, it is not a very good strategy because there is no control of the quality of template samples and therefore no control of the authentication performance of system. New references could be a bad presentation of biometric modality and on the contrary old template samples, which are a good representation of a modality, will be replaced. Anyway if it is required, that one template sample should be automatically replaced one time in a special period of time (e.g. monthly), this simple strategy can deal great improvement of authentication performance, and especially reducing of false rejections.



References
E_1
E_2
E_3
E_4

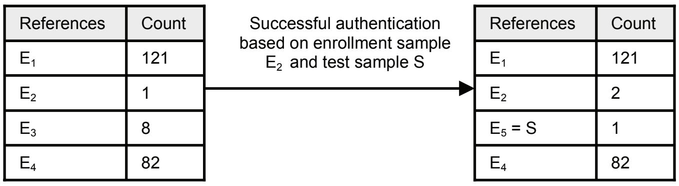
Successful authentication based on test sample S

References
E_2
E_3
E_4
E_5 = S

Figure 1. Template replacement scheme using FIFO

3.2 Least frequently used (LFU)

The least frequently used technique replaces the template sample, which was fewest number of times used for test sample authentication. In other words it counts how often an item is the nearest neighbor during authentications over a given time period and those that is used least often is discarded first. It is also not a very good strategy for replacement of biometric references because one of old templates can collect a lot of points in a short period of time, while person had some special appearance of biometric modality. Should the biometric modality of a person be changed in the future, this old and quite unlike template will not be discarded. On the other hand, if the replacement period is clearly defined (for instance one time in a month) and agrees with natural change of presentation of biometric modality, this strategy can be considered as useful for references replacement.



References	Count
E_1	121
E_2	1
E_3	8
E_4	82

Successful authentication based on enrollment sample E_2 and test sample S

References	Count
E_1	121
E_2	2
E_5 = S	1
E_4	82

Figure 2. Template replacement scheme using LFU

3.3 Least recently used (LRU)

Faced with having to replace a template sample at some point, then it should seem reasonable that the best template sample for a system to replace is the one that was not accessed for the longest time. Such a strategy would be applicatively for biometric template replacement. However, since the next used templates can not be predicted, such a system uses the assumption that the past will be a reasonable indication of the future and replaces the template sample that has been accessed least recently. This is known as least recently used (LRU) replacement algorithm. LRU (or LRU-like) is the nearly universal standard for cache replacement, which seems to be very hard to beat. If one want to make sure the algorithm always discards the least recently used item, it requires keeping track of what was used when, which is too expensive. Actually some probabilistic scheme is used, that almost always discards one of the least recently used items. Most of the currently used replacement policies (e.g., Clock algorithms) attempt to approximate LRU, diverging from it primarily for implementation efficiency reasons.

3.3.1 Clock algorithm

A promising cache replacement scheme for biometric reference sample replacement is the so called clock algorithm, a special case of the second-chance approach which is based on the FIFO replacement strategy. It works by maintaining a circular list of samples which are currently in reference storage. Consider each element in the list stores only a template sample number E_i and a reference value R_i, which is set to either 0 or 1, and i is the given number of template elements per user. In practice, each element contains other information as well. All templates initially have a reference value of $R_i=0$ and whenever one template sample is accessed by the system (found out as the best match), its reference value is set to 1. When an exchange of sample is needed, the system uses the circular list and the reference values R_i to determine which template sample should give up its position and have to leave the list. To determine this, it moves through the list until it finds a reference value of 0. As it traverses each template sample, the system resets the sample's reference value from 1 to 0. Once it encounters a 0, it has found a template sample that has not been accessed by the system since the last cycle through the list; thus, it is the reference vector least recently used. This template sample is then replaced with the new sample, and the new sample is inserted in place of the old template sample in the list. If all template samples have been accessed since the algorithm was last run, the system ends up making a complete cycle through the list and replaces the template sample at which it started. Figure 3 shows an example of working step of clock algorithm. Test sample S is successful matched with template sample E_4 and least recently used template sample E_3 is replaced by test sample S.

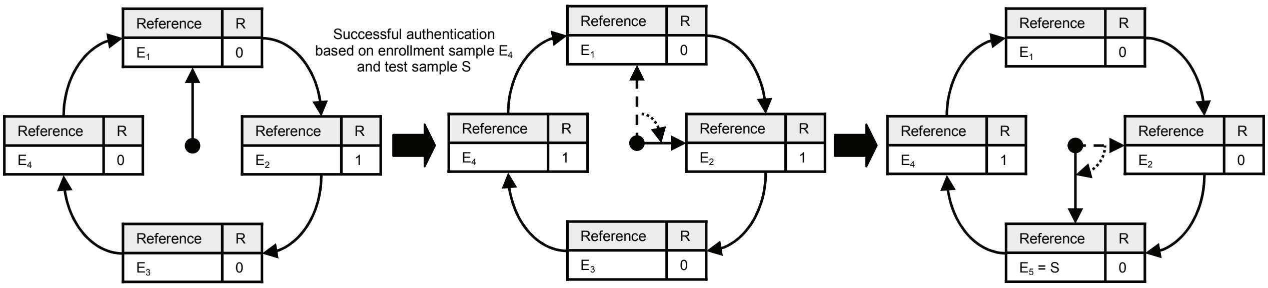
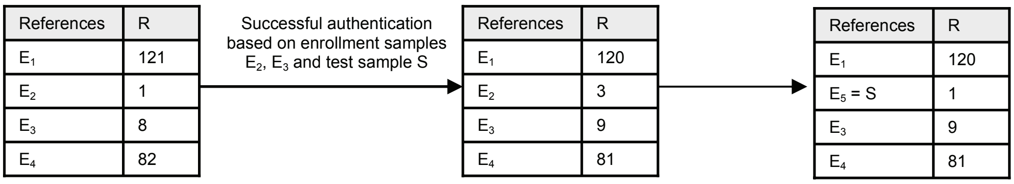


Figure 3. Template replacement scheme using Clock algorithm

3.4 Extended replacement algorithm

Considering special features of developed biometric systems a novel approach is proposed, which can be better applied for biometric reference sample replacement. To each template sample in the database an attribute R is added that shows the relevance of it. In the beginning every attribute is initialized with 0. Suppose after classification there are i best candidate templates with different matching scores. If these templates resemble the test sample in sufficient degree and the system decides this sample belongs to a legal person and could replace one of the template samples. The i best templates will be sorted in descending order and the relevance attribute of the first one will be increased by value i, relevance attribute of second by value i-1, relevance attribute of third by i-2 and so on. The template sample of authenticated person with the smallest relevance attribute will be discarded and test sample comes to its place. After every authentication the relevance attributes of all unused template samples will be decreased by 1. Based on this procedure a linear hierarchy of the template samples is created for each person in every moment of time, therefore the relevance of each template sample in hierarchy is defined by its relevance attribute R. By definition of least recently used template sample we take into account as well aging of template samples as frequency of use. Figure 4 shows an example of working step of the *extended replacement algorithm*. Template samples E_2 and E_3 are selected for authentication and whose relevance values are increased by 2 and 1 respectively. Then template sample E_2 with least relevance value is replaced by test sample S.



References	R
E_1	121
E_2	1
E_3	8
E_4	82

Successful authentication based on enrollment samples E_2, E_3 and test sample S

References	R
E_1	120
E_2	3
E_3	9
E_4	81

References	R
E_1	120
E_5 = S	1
E_3	9
E_4	81

Figure 4. Template replacement scheme using extended replacement algorithm

4. CONCLUSIONS AND FUTURE WORK

We realize that most biometric systems have a requirement to save collected template samples on read only mediums. This will be done for security reasons to protect reference storage from intruder's invasion and avoid a spoofing of biometric data. Dynamic templates management may cause the letdown of system security, but makes the biometric authentication system much more flexible. For identification systems, which usually have problems to recognize persons correctly because of intra-class variability and inter-class similarity and do not have very high security requirements, the using of dynamic templates can provide great performance improvement in sense of produced error rates. This work is now more theoretical and has an aim to show how cache replacement strategies can be adopted for the replacement of biometric template samples in order to hold it up-to-date. The introduced replacement strategies were implemented only for face recognition from video but sufficient testing was not done.

Further we intend also to produce these techniques for our signature verification system. In the future work the sufficient testing of authentication systems will be done and the reducing of error rates will be studied. Furthermore other replacement strategies (e.g. based on statistical Markov models [6]) and their application for template sample replacement will be considered.

ACKNOWLEDGMENTS

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507634 BIOSECURE. The studies on biometric template ageing were partly founded by the DFG (German Research Foundation). The content of this publication is the sole responsibility of the University Magdeburg and their co-authors and can in no way be taken to reflect the views of the European Union.

REFERENCES

1. Jain, A.K., Prabhakar, S., Ross, A. Fingerprint Matching: Data Acquisition and Performance Evaluation. MSU Technical Report TR99-14, 1999.
2. A. Ross, A.K. Jain, "Multimodal Biometrics: An Overview", Proc. Of the 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp. 1221 – 1224, 2004.
3. Scheidat, T., Vielhauer, C., Dittmann, J. Distance-Level Fusion Strategies for Online Signature Verification. In Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), Amsterdam, The Netherlands, 2005.
4. Tobias Scheidat; Andreas Engel; Claus Vielhauer: Parameter Optimization for biometric Fingerprint Recognition using genetic Algorithms; In: Proceedings of ACM 2006 Multimedia & Security Workshop, Geneva, Schwitzerland, 2006
5. Andrew S. Tanenbaum: Modern operating systems, Second edition, Prentice Hall PTR, 2001.
6. A.R. Karlin, S.J. Phillips, and P. Raghavan: Markov Paging, in Proc IEEE Symposium on the Foundations of Computer Science (FOCS), pp 208-217, 1992.