Experiments on Matching Intronized Fingerprint Minutiae Templates

Qinghai Gao[†], Xiaowen Zhang[††], and Michael Anshel[†††]

[†] Dept. of Computer Science, Graduate Center / CUNY, New York, NY, USA
[††] Dept. of Computer Science, College of Staten Island / CUNY, Staten Island, NY, USA
[†††] Dept. of Computer Science, City College of New York / CUNY, New York, NY, USA

Summary
Intronization, adding extra minutiae to the original fingerprint minutiae template, is tested for two different situations: verification (1:1) and identification (1:N). Our preliminary experimental results demonstrate that fingerprint minutiae templates intronized with different minutiae sets can still match with high selectivity. Therefore, intronization can be used to protect biometric templates.

Key words:
Intronization, verification, identification, security, biometrics.

1. Introduction

Biometric system works with two stages: registration and matching. During registration, a live biometrics will be measured and a template will be extracted and saved in a database. During matching, a new template will be obtained from the same live biometrics and then compared with the registered template.

Biometrics are used to verify and identify the input sample when compared to a template, in other words, they are used for verification and identification of humans upon their physical traits. Verification (1:1) means that for a person who claims to be someone, we will get a new biometric template from the person, which will be matched against a previously stored template of that someone in order to verify that he is who he claimed to. Identification (1:N) means that for an unknown person, we will obtain a new biometric template and then match the new template against many templates in database to see if there is a match to identify who he is.

To successfully implement biometric based authentication system, we have to find effective ways to protect biometric template. One-way hash function for password based authentication system does not work for biometrics due to the non-reproducibility of biometric measurements.

In this paper, we introduce a technique called intronization [1], which is a biological term referring to the accumulation process of introns in DNA. The existence of large number of introns in human DNA makes it mathematically difficult in predicting the boundary between exons and introns. From the perspective of security, we believe the protection due to the existence of introns may help organisms to survive. Inspired by the process in nature, we add some introns – a set of junk minutiae into a fingerprint minutiae template, and the expanded new minutiae template is said to be intronized. Since we only store the intronized templates in database, if the database is compromised the attacker has to identify the introns to retrieve the original fingerprint templates. Literature [4-8] proposed a fuzzy vault scheme to secure biometric template by adding chaff points to biometric templates. However, those chaff points have to be somehow recognized and separated from the real minutiae set later on. Unlike the fuzzy vault scheme, we strive to apply the intronized template directly – an effort to do hashing with noisy data. Our experimental results show that without removing introns from our intronized fingerprint template, the matching scores can still be satisfactory. Thus the intronization technique can be applied to protect the privacy of biometric information when deploy large biometric system.

The rest of the paper is organized as follows. In section 2, we perform verification (1:1) for various situations: templates with and without introns, same fingerprint with different sets of introns, similar or different fingerprints with different sets of introns. In section 3, we perform identification (1:N) for several cases: intronizing database only, intronizing probe fingerprint only, and intronizing both probe fingerprint and database. In section 4, we conclude the paper and lay out our future research.

2. Experimental Results on Verification (1:1)

Six fingerprints from FVC2004 database DB1 [3] are randomly selected. FP34_2a has 25 minutiae. Five minutiae of FP34_2a are significantly modified to obtain FP34_2b. All the minutiae of FP34_2b are slightly

[††] Corresponding author: X. Zhang
Manuscript received September 5, 2008
Manuscript revised September 20, 2008

modified to obtain FP34_2c. The matching scores for the fingerprints are given in Table 1.

Table 1 Matching scores for fingerprints from DB1 [3].

FP	1_1	8_2	34_2a	34_2b	34_2c	65_3	97_2	105_3
1_1	499	5	0	0	3	6	0	3
8_2		486	3	3	3	6	5	3
34_2a			103	62	54	6	3	0
34_2b				104	93	4	3	0
34_2c					104	3	3	3
65_3						499	3	12
97_2							136	5
105_3								219

The lower left triangle of Table 1 is left empty under the assumption of symmetrical matching scores.

To see how intronization changes matching scores we test six different situations.

2.1 With or Without Introns

FP34_2a, which has 25 original minutiae, is matched against itself inserted up to 50 introns from FP1_1. The results are given in Figure 1.

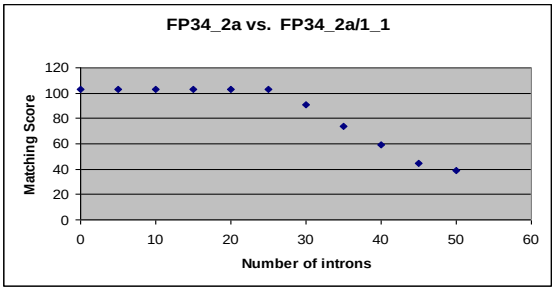


Fig. 1

From Figure 1, we can see that adding up to 25 introns has nearly no effect on the matching scores. However, adding 50 introns reduces the matching scores to 40, the threshold suggested by NBIS [2].

For FP34_2a we insert up to 80 introns from FP105_3 and 65_3, and match them against the original. The results are given in Figure 2.

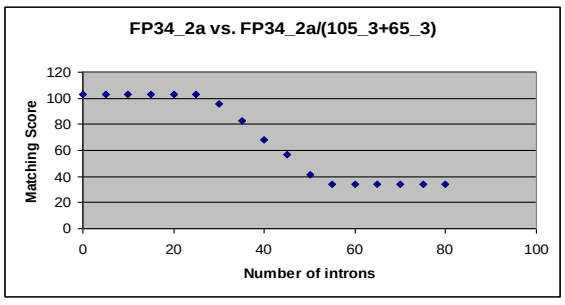


Fig. 2

FP34_2b, which has 25 original minutiae, is matched against itself inserted up to 50 introns from FP1_1. Figure 3 shows the results.

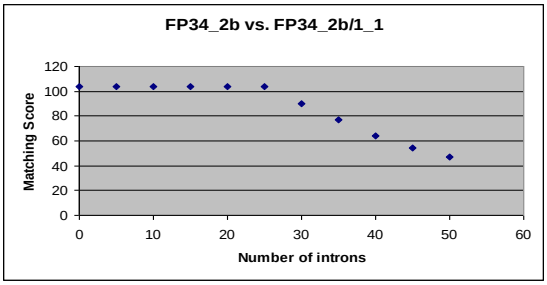


Fig. 3

FP97_2, which has 25 original minutiae, is matched against itself inserted up to 75 introns from FP1_1 and 8_2. Figure 4 shows the results.

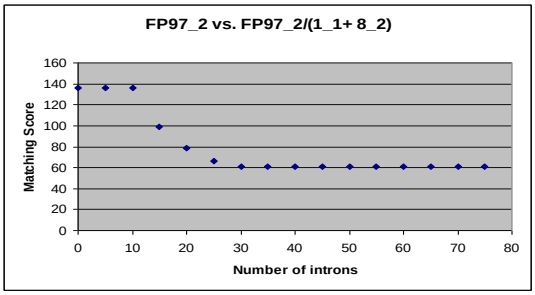


Fig. 4

The results from Figure 1 to 4 show that the intronization can be used as a hashing mechanism to protect fingerprints because the fingerprint templates inserted with certain number of introns can still match the original.

2.2 Same Fingerprint with Different Sets of Introns

For FP34_2a, we inserted the same numbers but two different sets of introns, and then match them against each other. The results are given in Figure 5.

From Figure 5 we can see that one fingerprint template inserted with one set of introns (From FP1_1) can still match itself inserted with a different set of introns (From FP105_3 and 65_3).

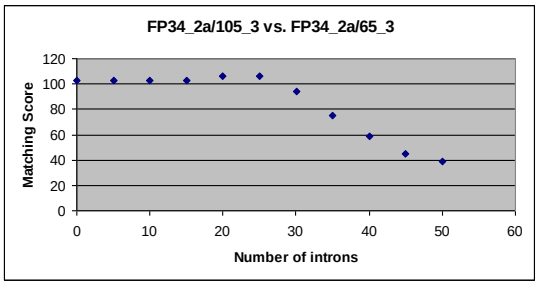


Fig. 5

2.3 Similar Fingerprints with Same Set of Introns

As shown in Figure 6, adding the same set of introns into FP34_2a and 34_2b the matching scores are increases, and so is the false matching rate.

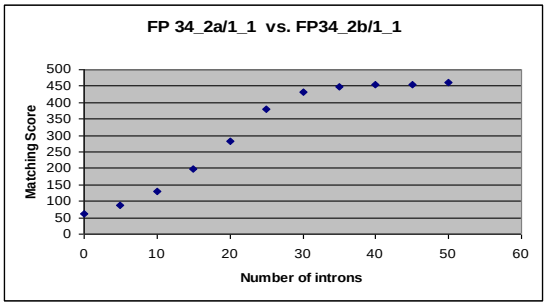


Fig. 6

2.4 Similar Fingerprints with Different Sets of Introns

Adding different sets of introns to FP34_2a and FP34_2b gives the results shown in Figure 7 and 8.

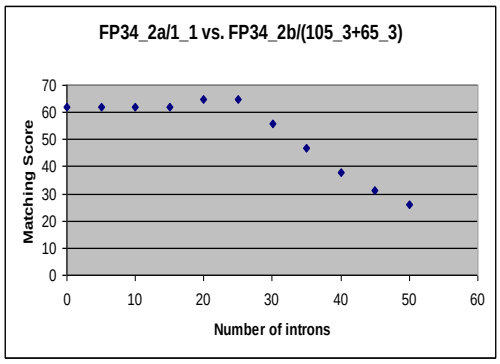


Fig. 7

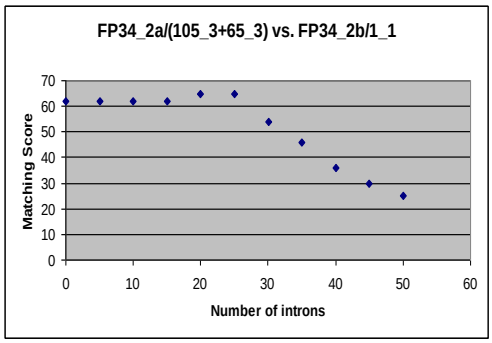


Fig. 8

In Figure 7 and 8, the intron sets are taken from FP105_3 first and then from FP65_3. Note that not all the minutiae of FP65_3 are used. Adding different sets of introns to FP34_2a and FP34_2c the results are shown in Figure 9 and 10.

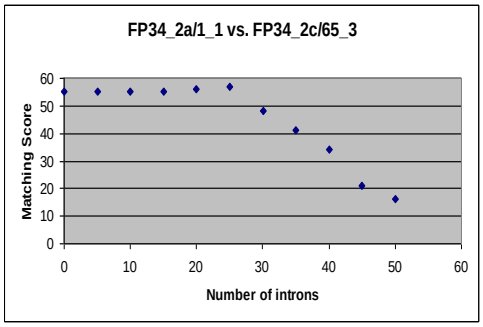


Fig.9

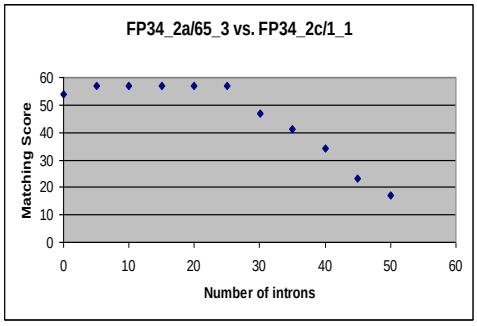


Fig. 10

The results from Figure 7 to 10 show that similar fingerprints inserted with different sets of introns may still match, which provides a solution to the non-reproducible problem of biometrics.

2.5 Different Fingerprints with Same Set of Introns

For different fingerprints, adding the same set of introns will significantly increase the false match rate, as illustrated in Figure 11.

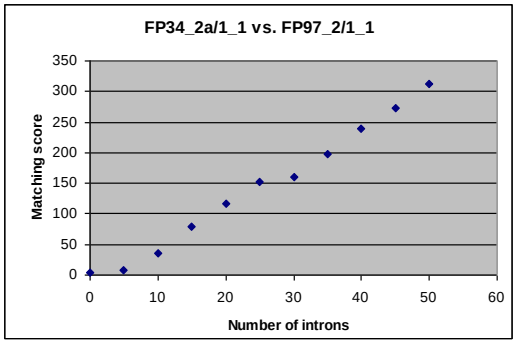


Fig. 11

From Figure 6 and 11, we conclude that it should be avoided to add the same set of introns to different fingerprints.

2.6 Different Fingerprints with Different Sets of Introns

Two different fingerprints and two different sets of introns are used. The results are given in Figure 12 and 13.

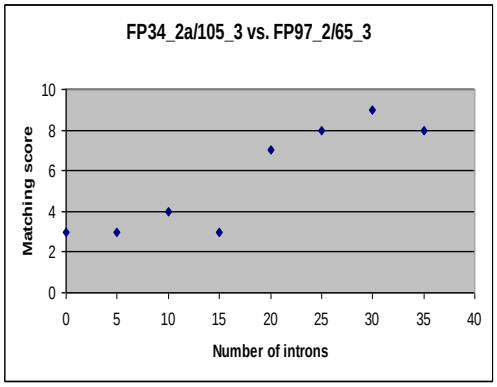


Fig. 12

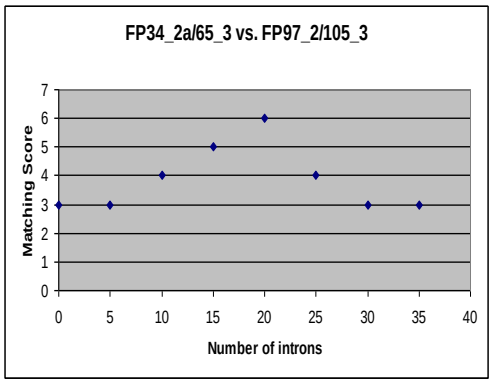


Fig. 13

From Figure 12 and 13, we can see that adding different sets of introns to different fingerprints does not significantly change the matching scores.

In sum, the results from Figure 1 to 13 support the following observations:

- intronization can be used as a hashing mechanism for protecting biometrics.
- Different sets of introns should be used for same or similar fingerprints.
- Increasing the similarity of two fingerprint templates may allow a larger Message Expansion Rate.
- Avoid using the same set of introns.
- Adding different sets of introns to different fingerprints will not significantly change the matching score.

Based on these results, we choose to test adding different sets of introns to different fingerprints as given in section 3.

3. Experimental Results on Identification (1:N)

Depending on where to add introns, probe fingerprint or database, three situations are considered as shown from section 3.1 to 3.3.

3.1 Intronize database only

All of the intron sets are different. Figure 14 shows the results.

In Figure 14, every graph follows a similar distribution with a peak matching score smaller than 5, and none of the matching scores is greater than 20. According to the threshold 40 [2], the false matching rate is 0.

In database DB1, there are 880 fingerprints. Figure 14 only shows 879 of them. The matching score for the remaining probe fingerprint 34_2 against itself is given in Table 2.

Table 2 Matching scores for probe fingerprint FP34_2.

# Introns	0	5	10	15	20	25
Matching Score	103	103	103	103	103	41

Table 2 tells us that the false non-matching rate is 0 with up to 25 introns. Most importantly, the data in Table 2 follows similar pattern as those in Figure 1 and 2.

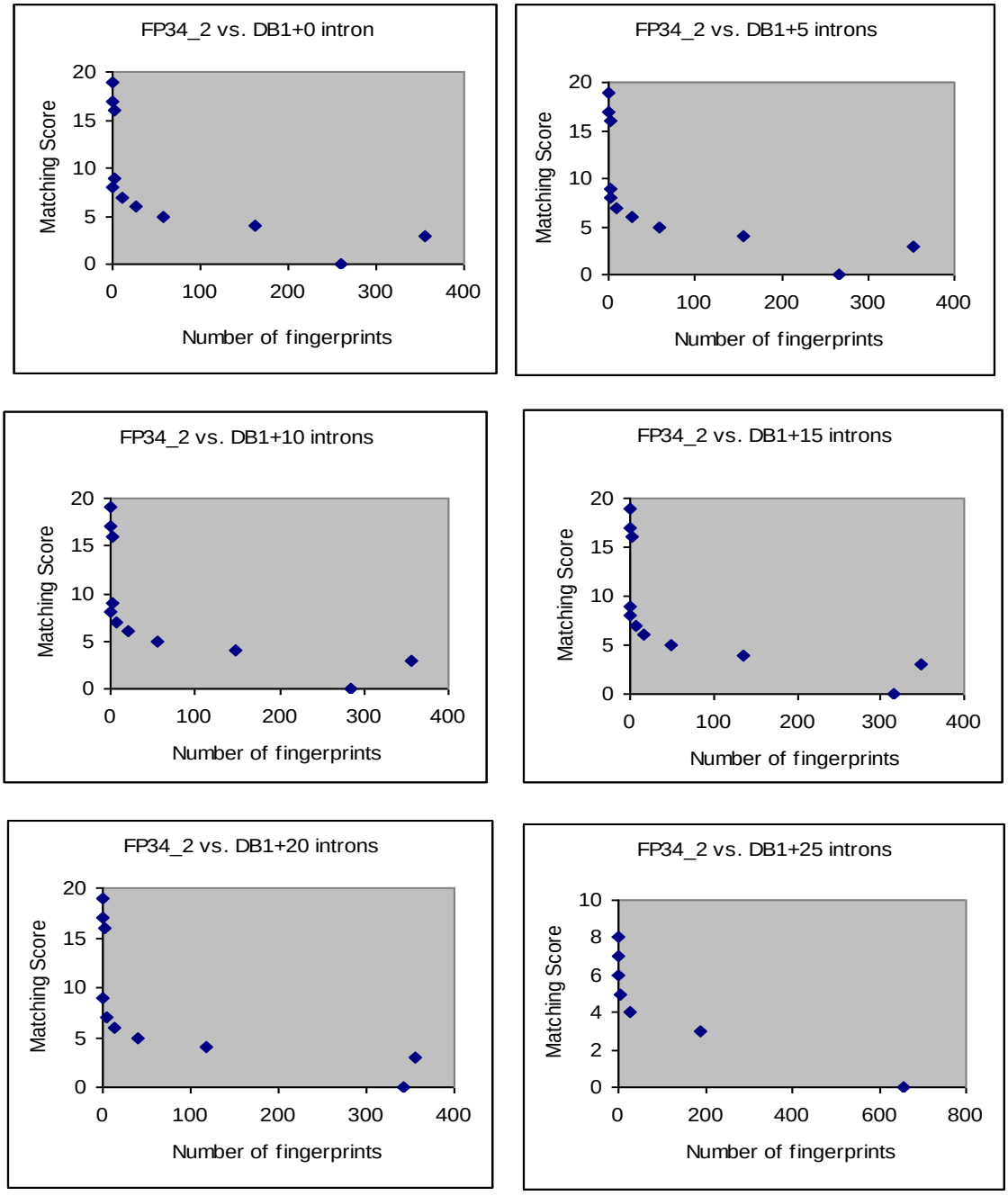


Fig. 14 Intronize database only.

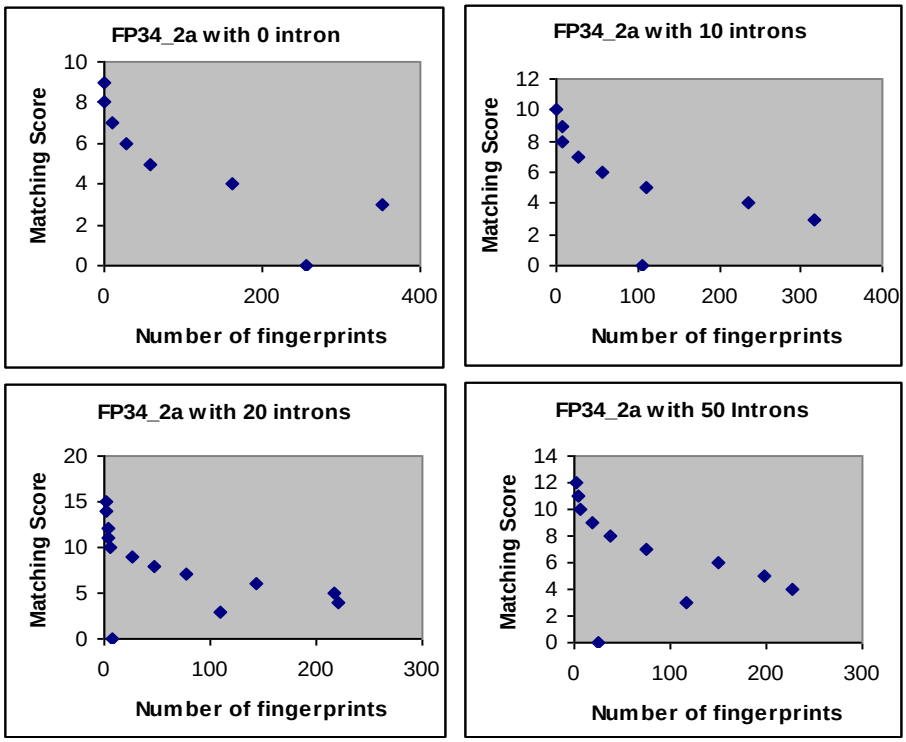


Fig. 15 Intronize probe fingerprint only.

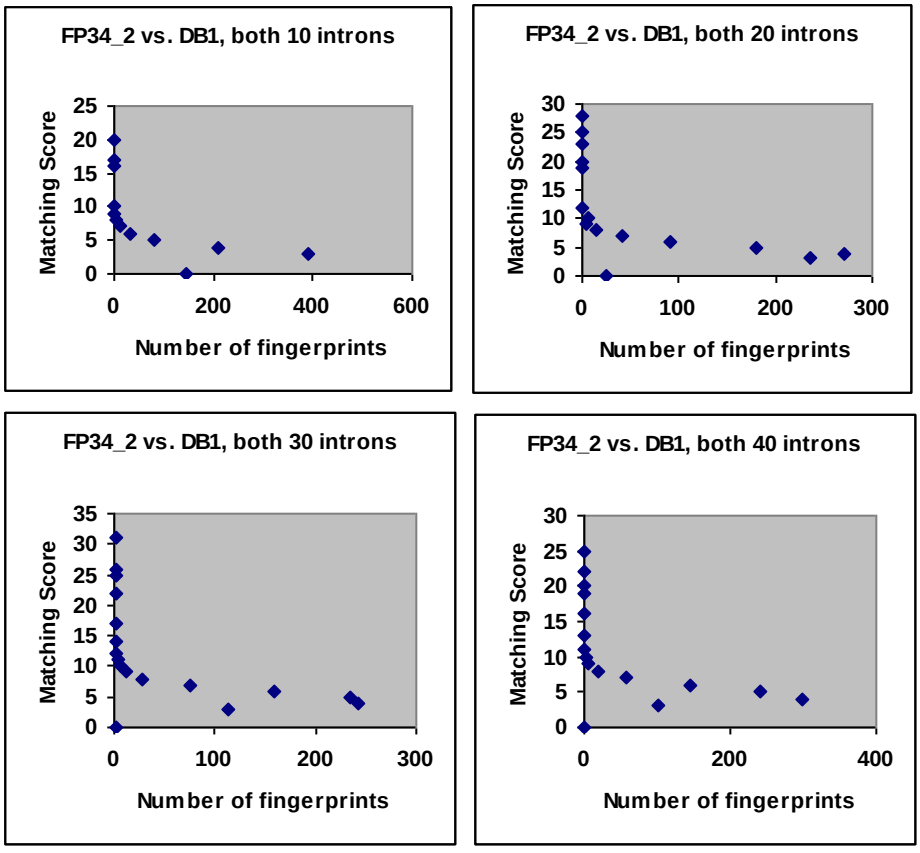


Fig. 16 Intronize both probe fingerprint and database.

3.2 Intronize probe fingerprint only

The sets of introns for probe fingerprint FP34_2 are obtained from FP1_1. We modified the database DB1 by removing the fingerprints that are related to the probe fingerprint, including 16 fingerprints from FP1_1 to 1_8 and FP34_1 to 34_8. Therefore only 864 fingerprints are left for testing. The results are given in Figure 15.

From the matching scores represented by the Y-coordinate, we can see that the peak values are around 5 and the maximum values are less than 20. Therefore, the false matching rate is 0.

3.3 Intronize both probe fingerprint and database

There are 879 fingerprints. All of intron sets are different.

Figure 16 shows the testing results as we add up to 40 introns (MER > 2) to both probe fingerprint and database fingerprints.

Table 3 gives the matching results of FP34_2 against FP34_1 to 34_8 during the intronization process.

Table 3 Matching results for FP34_2 inserted up to 40 introns.

	0	5	10	15	20	25	30	40
34_1	4	4	4	0	8	5	5	5
34_2	103	148	147	192	241	320	320	499
34_3	17	17	17	17	28	31	31	25
34_4	9	9	10	10	10	10	10	5
34_5	16	16	16	23	23	24	25	19
34_6	19	19	20	20	20	20	22	22
34_7	16	16	17	17	25	26	26	16
34_8	3	11	5	16	19	17	17	20

From Figure 16 and Table 3, we can see both the false match rate and the false non-match rate are equal to 0%. These results again show that the intronization technique can be used as an effective method for protecting fuzzy biometrics.

4. Conclusions and Future Research

Our preliminary results by using NBIS [2] and FVC2004 Fingerprint databases [3] show that randomized intronization to database of fingerprint templates can be used as a secure mechanism to protect original templates. Without removing introns (randomly added minutiae) the matching scores for verification (1:1) and identification (1:N) are still acceptable.

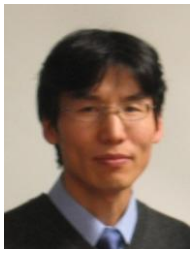
In the future we would like to devote our time to the following two directions:

1) More advanced intronization techniques – Nature has created many algorithms that deserve computer scientists to explore. Two terms from Genetics, Alternative Splicing and Restriction Enzymes, could be the starting points for advanced intronization algorithm design.
2) Better matching algorithm design – The matching algorithm used here is based on line segments. Different matching algorithms can be designed, such as triangular matching.

References

[1] Qinghai Gao. *Secure Biometrics*. PhD thesis (2008), City University of New York.
[2] NIST Biometric Image Software (NBIS). Available at: http://fingerprint.nist.gov/.
[3] FVC2004 Fingerprint databases are used. Available at: http://bias.csr.unibo.it/fvc2004/.
[4] A. Juels, M. Wattenberg. “A Fuzzy Commitment Scheme”. Proc. ACM Conf. Computer and Communications Security, 1999, pp. 28–36.
[5] A. Juels and M. Sudan. “A Fuzzy Vault Scheme”. IEEE International Symposium on Information Theory, 2002.
[6] T. C. Clancy, N. Kiyavash, and D. J . Lin. “Secure smartcard-based fingerprint authentication,” Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pp. 45-52.
[7] U. Uludag and A.K. Jain. "Fuzzy Fingerprint Vault", Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice, pp. 13-16, Cambridge, UK, August 2004.
[8] U. Uludag, S. Pankanti and A. Jain. "Fuzzy Vault for Fingerprints", Proc. of Audioand Video-based Biometric Person Authentication (AVBPA) 2005, pp. 310-319, Rye Brook, NY, July 2005.

Dr. Qinghai Gao currently works in the IT department of Linear Lighting Corporation in New York. His present research interests include Biometrics, Biological Information System, Cryptography, Polymorphic virus and Network Security. He received a PhD in Computer Science from the City University of New York in December 2007.



Dr. Xiaowen Zhang is a faculty member of the College of Staten Island (CSI). Prior to joining CSI, he worked in both academia as a research fellow and lecturer, and industry as a software and electronic engineer. His research interests include information security, cryptography, RFID, quantum computing, and wireless communications. He received a PhD in Computer Science from the City University of New York (CUNY), New York, USA in 2007, and a PhD in Electrical Engineering from Northern Jiaotong University, Beijing, China in 1999.

Dr. Michael Anshel has taught at the City College of New York (CUNY) since 1968. He has been a member of the CUNY Doctoral Faculty since 1973, teaching in the Engineering, Computer Science and Mathematics programs. He has mentored over forty doctoral dissertations. Dr. Anshel is co-inventor of three patents in cryptography and has published numerous articles in Mathematics and Cryptography. Dr. Anshel is a member of the AMS, MAA, ACM, IEEE, IACR. Dr. Anshel holds a Ph.D. in Mathematics from Adelphi University in Garden City, New York.