

A NOVEL METHOD TO IDENTIFY HUMAN FINGERPRINTS

¹AHMAD SHARADQH

¹Al-Balqa Applied University, Computer Engineering Dept., Jordan

E-mail: ¹dr.ahmed.sharadqah@bau.edu.jo

ABSTRACT

Human fingerprints unique signature among each person. Hence, the requirement for fingerprint identification among a different pattern of human fingers is a crucial security issue. Since fingerprint features are vary from one person to another, a detail of any person can be acquired by recognize the fingerprint features. These features are used as a key to retrieve any information connected to the human. This research proposal will argue the existing fingerprint method, extract fingerprints features and build a data base of the features. The performance issues will be calculated, and the identification process accuracy will be measured. A novel method of fingerprint feature extraction will be proposed, implemented and tested. The obtained experimental results will be compared with other methods results to prove the proposed method advantages.

Keywords: *Fingerprint, identifier, cluster, centroid, WCS, LBP, CSLBP.*

1. INTRODUCTION

Human fingerprint considered to be a substantial factor for human identification. There are number of schemes used to examine the fingerprints with the intention of identifying the person. Many techniques are based on extracting features values, which forms a small key for recognition purposes. These unique features found within the patterns make us capable of giving opinion. The classical method of fingerprint is a time-consuming procedure needs to be revised.

In this research proposal an efficient and highly accurate method for identifying fingerprint will developed. The proposed method will base on Laplacian equation to detect local extremes in the fingerprint image, these local extremes will for the features key to be used later on for identification purposes. The extracted features will be saved and stored in a features database; this data base will be passed to a neural network for recognition purposes.

The objective of this research will be focused on the following:

1. developing a novel method for fingerprint identification
2. Examining existing method.
3. Experimental investigation of the proposed method.

4. Comparing the proposed method results with other methods result for accuracy and performance issues.

Fingerprint identification is a process of creating small in size array of features, which must be a unique and can be used as a signature or key to retrieve, identify or recognize the human. The process of fingerprint identification is a vital one due to the huge variety of application requiring this process; Biometric technology can be used for a great number of applications. Chances are, if security is involved, biometrics can help make operations, (see figure 1) transactions and everyday life both safer and more convenient. Here you will find a list of the many areas of deployment for biometrics and the companies that provide applicable identity solutions:



Figure 1: Biometric transaction.

Biometric Security, border control/airports, consumer/residential biometrics, financial biometrics, fingerprint & biometric locks, healthcare biometrics, Justice/law enforcement, logical access and Mobile biometrics.

2. LITERATURE REVIEW

A model for processing of fingerprint is explained based on ridges manipulation, where the Ridge boundaries turn out to be much flatter. However, some difficulties need to be resolved especially when the image regions are corrupted with dense noise [1].

The performance of fingerprint-based system which using the modified Gabor filter is outstanding especially for noisy images with corrupted ridges. However, this scheme has a drawback in terms of speed and efficiency [2].

A unique strategy for finger print recognition uses a convolution of the picture with Gabor channels. The main part of this methodology includes standardization, edge estimation and filtering [3].

A method to create dummy fingers has been proposed, in this approach several fingerprints has been tested to check whether they accept a dummy finger instead of a real finger [4].

A novel digital watermarking method is used to improve the security of fingerprints using demographic text data as various watermarks for verifying the protection of a fingerprint image. The degree of similarity between the embedded images and the extracted images is calculated using pixel-based metrics. Hence, added protection from interfering is achieved [5, 6].

A Fingerprint aliveness detection method using local ridge frequencies is proposed. This method needs more than one image for performing the aliveness check. In this work, a livens measure based on single image is developed. The essential density differences between 'live' and 'not live' fingerprint images are achieved [7].

A comprehensive methodology to Biometric Cryptographic Keys security evaluation is achieved. This evaluation includes existing BCKs and it has been found that the analysis of their security is insufficient. Moreover, the error rates, the randomness of biometric features and the generated key size are evaluated [8].

The process of fingerprint identification as shown in figure 2 is based on a created database of fingerprints features (identifiers), and the process of identification requires two phases:

- Enrolment phase, to create features and to add them to features database.
- Matching or recognition, to create features and search the database to find the similar (if exists).

So, we can summarize the process of identification in the following steps:

1. Performs transmission/reception of the security data.
2. Performs creation of security data and update of database using the Fingerprint Recognition Setting Tool.
3. Performs security data creation and update of database using the display unit (from offline mode or from created screens).

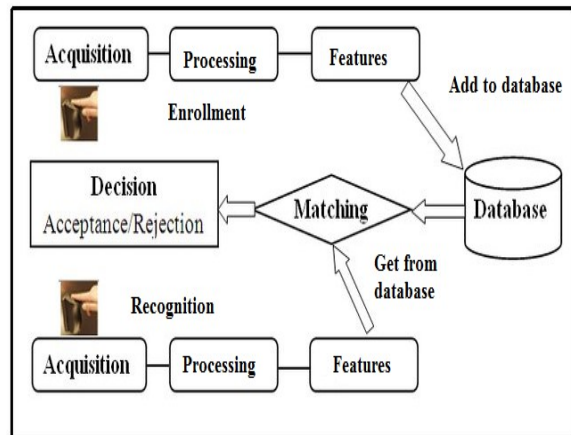


Figure 2: Identification process

Figure 3 shows the required steps performed in biometric security system:

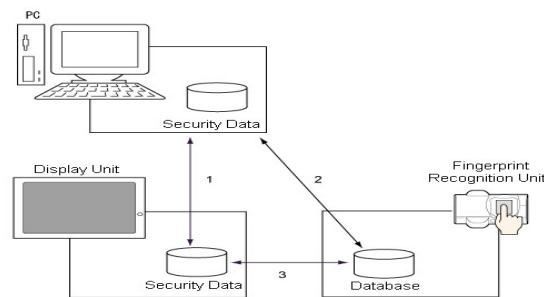


Figure 3: Biometric security system

1. Touch the fingerprint recognition unit to verify with the fingerprint database.
2. Search from matching fingerprint in the security data.
3. Login using the registered user ID/password/level.

Many authors used the local binary pattern (LBP) based methods to create unique features for each fingerprint [9].

Features extraction LBP based methods calculate the LBP operator for each pixel as shown in Fig. 4, this method produces an array features of 256 elements, this array is too big to be used as a fingerprint identifier requiring more memory space to be store in and more extraction and identification time [10], [11].

Center-symmetric (CSLBP) method is one of popular versions of LBP methods, it reduces the element of features array to 16, thus reduces the memory space size and the extraction time, CSLBP can be calculated for each pixel as shown in Fig.4.

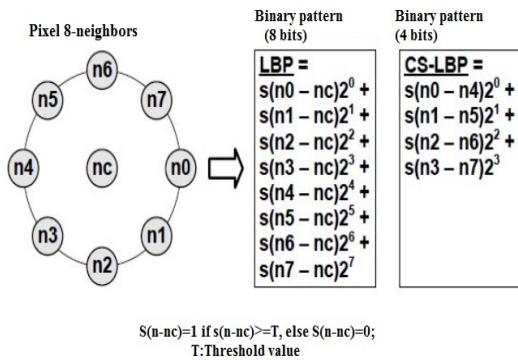
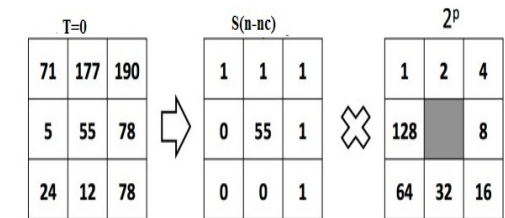


Figure 4: LBP and CSLBP calculation

Fig. 5 shows an example of calculation LBP operator for a selected pixel:



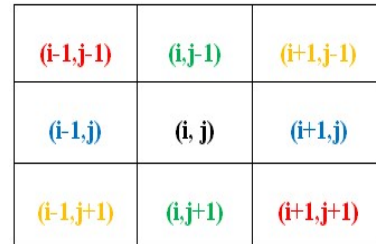
$LBP=1 \times 1 + 1 \times 2 + 1 \times 4 + 1 \times 8 + 1 \times 16 + 0 \times 32 + 0 \times 64 + 0 \times 128 = 4 + 8 + 16 = 31$

Figure 5: LBP calculation example

In this research we will propose a reduced LBP (RLBP) method, which creates array features of 8 elements, each element value points to the repetition of one of the numbers 0 to 7, the features array can be calculated as shown in Fig. 6, This method has the following features:

1. The number of features is reduced to 8.
2. It requires less memory space and less extraction and identification times.
3. For each fingerprint the extracted features are unique, thus we can use them as a fingerprint identifier.

The disadvantage of RLBP method is sensitivity, any changes in the fingerprint position will lead to generate a new features array, considering the rotated fingerprint as a new fingerprint adding a big efforts to the process of fingerprint identification, this disadvantage will be solved by introducing the proposed latter in this research novel method.



$$\begin{aligned}
 a &= ((I(i, j+1) - I(i, j-1) > T) * 2^0); \\
 b &= ((I(i+1, j+1) - I(i-1, j-1) > T) * 2^1); \\
 c &= ((I(i+1, j) - I(i-1, j) > T) * 2^2); \\
 d &= ((I(i+1, j-1) - I(i-1, j+1) > T) * 2^3); \\
 e &= a+b+c+d; \\
 h(e+1) &= h(e+1) + 1;
 \end{aligned}$$

Figure 6: RLBP calculation

3. PROPOSED NOVEL METHOD

Fingerprints are usually represented by a 2D matrix (Gray fingerprints) [12], or a 3D matrix (Color fingerprint: one dimension for each color: red, green and blue) [13], [14]. The proposed novel method of fingerprint is based on C_mean clustering with some modifications [15], [16], here a fingerprint data set must be normalized and minimized by getting the fingerprint histogram [14], and to do this we can apply the following procedures:

- If the fingerprint is a gray one, calculate the histogram to be used as an input data set to C_mean clustering method.

If the fingerprint is a color one, then select one of the following options:

1. Reshape the 3D matrix to 2D matrix, and then calculate the histogram to be used as an input data set.
2. Convert the color fingerprint to gray, and then calculate the histogram of the gray image to be used as an input data set.
3. For each color, calculate the histogram, and then add the 3 histograms to get the total histogram to be used as an input data set.

Fig. 7 shows a color fingerprint and the corresponding histograms:

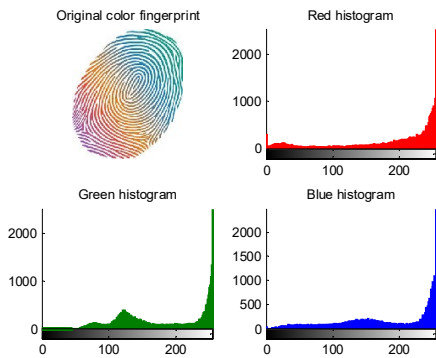


Figure 7: Color fingerprint histograms

Using fingerprint histogram will give us the following advantages:

1. Minimizing the input data set thus will minimize the required clustering time.
2. Rotating the fingerprint image does not affect the histogram, thus the features of the fingerprint will be fixed and stable, even if we rotate the fingerprint.

Clustering means grouping the data items in the input data set into clusters as shown in Fig. 8 and 9.

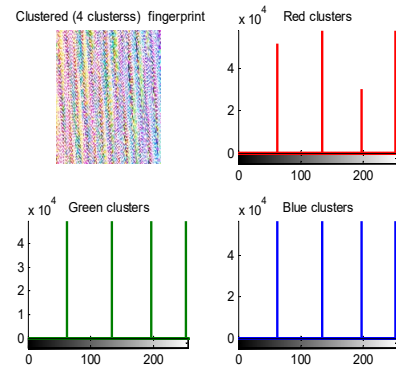


Figure 8: Dividing fingerprint into 4 clusters

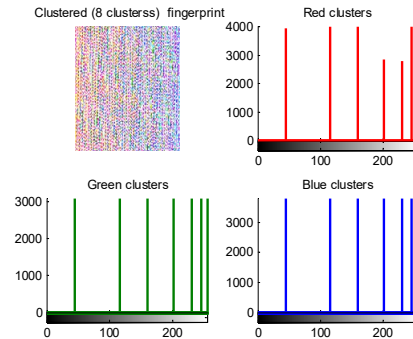


Figure 9: Dividing fingerprint into 8 clusters

C_mean method [15], [16] for fingerprint features extraction is a flexible method because of the following reasons:

- The number of clusters is variable, so the number of features is also variable.
- We can use the clusters centroids, or a within clusters sums (WCS), or number of points in each cluster as fingerprint features.
- Fingerprint features are fixed, and they do not depend on the image position.

The proposed method of fingerprint features extraction can be applied implementing the following steps:

1. Fingerprint capturing.
2. Input data set (histogram) normalization.
3. Initialization: Select the number of clusters, and the centroid of each cluster.
4. While there are changes in the centroid's values do the following:
 - a. Calculate the absolute value of distance between each data item value and each

- centroid.
- b. Append the data item to the nearest cluster depending on the distance.
- c. Find the new centroid value by averaging the data items within the cluster.

Worked Example:

Suppose we have the following input data set: 1, 3, 4, 9, 11, 13, 14, 15 And we want to group it into two clusters with initial centroids: c1=1, c2=5.

Tables 1 and 2 show the process of calculation.

Tables 1: Round 1

Data set	Distant 1	Distant 1	Nearest cluster	New centroid
1	0	4	1	C1=2 C2=9.8571
3	2	3	1	
4	3	1	2	
9	8	3	2	
11	10	5	2	
13	12	8	2	
14	13	9	2	
15	14	10	2	
Round 1				

Tables 2: Round 2

Data set	Distant 1	Distant 1	Nearest cluster	New centroid
1	1	8,8571	1	C1=2.67 C2=12.4
3	1	6,8571	1	
4	2	5,8571	1	
9	7	0,8571	2	
11	9	1,1429	2	
13	11	3,1429	2	
14	12	4,1429	2	
15	13	5,1429	2	
Round 2				

Tables 3: Round 3











4. IMPLEMENTATION AND EXPERIMENTAL RESULT



To analyze the proposed and the LBP based methods of fingerprints features extraction, and to do some comparisons between them we execute the following experiments:



Experiment 1: Using c_mean clustering with four clusters.

Several fingerprints were taken, a MATLAB code using the proposed method was written and executed using each of the selected fingerprints, and table 3 shows the results of execution by initializing the number of clusters to four clusters:

Table 3: Fingerprints features using four clusters

No	Fingerprint	Four Clusters (features)			
1.		252	184	98	9
2.		253	188	101	24
3.		251	185	99	12
4.		250	183	99	9
5.		252	190	110	13
6.		253	190	106	12
7.		245	175	89	3
8.		250	187	108	14
9.		246	183	102	9
10.		253	204	145	79



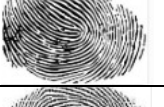


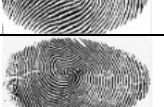

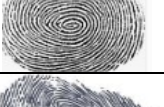

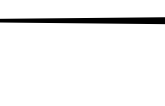
11.		251	190	108	16
12.		253	185	96	8

11		252	191	108	16
12		254	186	97	9

From table 3 we can see that the features for each fingerprint are unique, thus we can trust this method to form a fingerprint features to be used as an identifier to retrieve or recognize the human fingerprint.

Experiment 2: Using C_mean clustering to form the features for the rotated fingerprints.

Table 4: Features for fingerprints with rotation right 90 degrees

No	Fingerprint	4 Clusters (features)			
1		252	184	98	9
2		253	188	101	24
3		251	185	99	12
4		250	183	99	9
5		252	190	110	13
6		253	190	106	12
7		245	175	89	3
8		250	187	108	14
9		246	183	102	9
10		253	204	145	79

In this experiment we took the same fingerprints and rotate each of them 90 degrees to the right, and then the proposed method was applied; table 4 shows the results of executing this experiment.

From table 4 we can see that the features remain the same as in table 3, which give us an advantage of fixing the fingerprint features even if we rotate it.

Experiment 3: Varying the fingerprint resolution.

Here in this experiment we acquired a fingerprint with various resolutions, and the applied the proposed method to extract the fingerprint features, table 5 shows the results of executing this experiment:

Table 5: Fingerprint 1 features with various resolutions

Resolution	Clusters (features)				Extraction time (seconds)
600x385 x1	252	184	98	9	5.123000
1300x1009 x3	252	184	98	9	28.794000
368x267x1	252	184	98	9	2.145000
265x190x1	252	184	98	9	1.096000
283x178x1	252	184	98	9	1.167000
500x355x3	252	184	98	9	3.955000
1079x650x3	252	184	98	9	15.875000
280x180x3	252	184	98	9	1.093000

From table 5 we can see that the features remain the same, but high-resolution fingerprints require more extraction time.

Experiment 4: Using alternative features.

As we said earlier, we can use WCS as alternative features for each fingerprint, the tables 6, 7, and 8 show the results of implementing this experiment:

Table 6: Using WCS as features (8 clusters)

Table 7: WCS for rotated fingerprint 1

Table 8: WCS for fingerprint I with different resolutions

Here we can prove that we can use WCS instead of clusters centroids without losing any thing.

Experiment 5: Using LBP based methods to extract fingerprint features.

Here we took 6 fingerprints and apply CSLBP method to form fingerprint features, tables 9 and 10 show the results of implementing this experiment:

Table 9: Fingerprint features using CSLBP method

Fingerprints features					
F16	F17	F18	F19	F20	F21
33195	80116	37238	14458	72605	55555
7706	4638	5887	9905	4581	6857
2553	2469	3430	2202	2777	2592
16046	8071	15710	15859	7074	13271
8072	4821	9203	11925	7562	6492
8339	4879	7091	9822	7325	5223
2213	1833	2570	2523	2345	1801
11212	6233	10754	12058	5258	9376
14737	10879	18199	17097	6576	14333
2046	1446	2082	2495	2533	1442
8356	4941	6963	9889	7819	5185
6591	3471	6424	11260	7316	4587
15063	5400	10602	12719	5733	9835
1706	1199	1833	1594	2146	1448
6766	5876	4623	9139	4031	5836
5049	3136	6354	6018	3279	5678

Table 10: Rotated 90 degrees fingerprint features using CSLBP method

Fingerprints features					
F16	F17	F18	F19	F20	F21
20229	69766	38983	14635	52761	43069
7681	6714	9629	8377	7503	6104
3016	3019	3260	1812	4127	3755
22189	10437	14373	13328	15325	17278
14338	16752	7903	13390	5237	7809
5455	2711	5790	14090	3586	5391
2270	1310	2557	2366	2172	1836
12775	3080	10953	11385	8340	12200
23119	11673	17204	16425	15273	23060
1848	1700	2007	2447	3380	1332
6742	8176	5510	14138	6442	4867
6582	4749	5487	12362	6833	4702
12809	3819	10443	10704	10234	9736
1449	896	1884	1254	1502	1036
4573	2834	8062	6939	3002	3965
4723	1936	5286	5679	3467	3723

From tables 9 and 10 we can see that CSLBP methods form unique features for a fingerprint, but if we rotate the fingerprint the feature will change, adding troubles for a fingerprint identification system.

5. CONCLUSION

A method of fingerprint features extraction was proposed, tested and implemented, based on the obtained experimental results we can raise the following facts:

- The method produces a unique identifier (features) for each fingerprint.
- The features remain the same (are fixed and stable) for various rotated versions of the original fingerprint.
- The features remain the same (are fixed and stable) for various resolution versions of the original fingerprint.
- There is an alternative variant of the extracted features.

REFERENCES:

[1] Han Y, Ryu C, Moon J, Kim H, Choi H. "A study on evaluating the uniqueness of fingerprints using statistical Analysis", *International Conference on Information Security and Cryptology*, 2004, pp. 467-477.

[2] Zwiesele A, Munde A, Busch C, Daum H. "BioIS study. Comparative study of biometric identification systems", *Proceedings IEEE 34th Annual 2000 International Carnahan Conference on Security Technology*, 2000, pp.60-63.

- [3] Espinoza M, Champod C, M argot P. "Vulnerabilities of fingerprint reader to fake fingerprints attacks", *Forensic Science international*, Vol. 204, No. 1, 2011, pp. 41-49.
- [4] Espinoza M, Champod C. "Risk evaluation for spoofing against a sensor supplied with livens detection", *Forensic science international*, 2011, pp.162-168.
- [5] Galbally J, Fierrez J, Alonso-Fernandez F, Martinez-Diaz M. " Evaluation of direct attacks to fingerprint verification systems", *Telecommunication Systems*, Vol. 47, 2011, pp. 243-254.
- [6] Kang H, Lee B, Kim H, Shin D, Kim J. "A study on performance evaluation of the livens detection for various fingerprint sensor modules", *In International Conference on Knowledge - Based and Intelligent Information and Engineering Systems*, 2003, pp.1245-1253.
- [7] Van der Putte, Keuning J. "Biometrical fingerprint recognition: don't get your fingers burned", *Smart Card Research and Advanced Applications*, 2000, pp. 289-303.
- [8] Matsumoto T, Matsumoto H, Yamada K, Hoshino S. "Impact of artificial gummy fingers on fingerprint systems", *Electronic Imaging*, 2002 Apr 18, pp.275-289.
- [9] Zahran Bilal and Al-Azzeh, Jamil and Alqadi Ziad and Al Zoghoul, Mohd-Ashraf, "A Modified LBP Method To Extract Features From Color Images" , *Journal of Theoretical and Applied Information Technology*, Vol. 96, No. 10, 2018, pp. 3014-3024.
- [10] Mohd-Ashraf Zoghoul, Saleh Khawatreh, Zaid Alqadi, "Efficient Methods used to Extract Color Image Features", *IJCSMC*, Vol. 6, No. 12, 2017, pp 7-14.
- [11] Belal Ayyoub, Jihad Nader, Ziad Alqadi, Bilal Zahran, "Suggested Method to Create Color Image Features Victor", *Journal of Engineering and Applied Sciences*, Vol. 14, No. 1, 2019, pp 2203-2207.
- [12] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A.Abu Jazar and Rushdi Abu Zneit, "Optimized True- RGB color Image Processing", *World Applied Sciences Journal*, Vol. 8, No. 10, 2010, pp. 1175-1182.
- [13] A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using A New R'G'I Model", *journal of Computer Science*, Vol. 5, No. 4, 2009, pp. 250-254.
- [14] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata, "Creating a Color Map to be used to Convert a Gray Image to Color Image", *International Journal of Computer Applications*, Vol. 153, No. 2, 2016, pp. 31 – 34.
- [15] Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, "Creating a Stable and Fixed Features Array for Digital Color Image", *IJCSMC*, Vol. 8, No. 8, 2019, pp. 50 – 62.
- [16] Ahmad Sharadqh, Jamil Al-Azzeh, Rashad Rasras, Ziad Alqadi, Belal Ayyoub, "Adaptation of matlab K-means clustering function to create Color Image Features", *International Journal of Research in Advanced Engineering and Technology*, Vol. 5, No. 2, 2019, pp. 10-18.

Table 3: Round 3

Data set	Distant 1	Distant 1	Nearest cluster	New centroid	So, the centroids are: C1=2.67 C2=12.4 WCS1=8 WCS2=62 Number of points: 35
1	1.6700	11.4000	1	C1=2.67	
3	0.3300	9.4000	1		
4	1.3300	8.4000	1		
9	6.3300	3.4000	2	C2=12.4	
11	8.3300	1.4000	2	No change	
13	10.3300	0.6000	2		
14	11.3300	1.6000	2		
15	12.3300	2.6000	2		
Round 3					

Table 6: Using WCS as features (8 clusters)

Fingerprint number	Within_cluster sums							
	WS1	WS2	WS3	WS4	WS5	WS6	WS7	WS8
1	164	270	397	543	691	868	1114	1369
2	195	283	413	566	790	1045	1305	1560
3	167	273	400	547	695	864	1125	1380
4	171	272	397	541	718	930	1140	1427
5	186	282	411	565	732	908	1111	1398
6	172	272	410	561	721	892	1083	1398
7	159	251	376	512	875	1135	1518	1773
8	170	279	408	559	709	909	1125	1405
9	171	265	392	540	781	974	1224	1479
10	199	339	505	681	887	1079	1355	1681
11	198	293	422	565	745	944	1114	1446
12	187	268	402	542	740	904	1159	1419

Table 7: WCS for rotated fingerprint 1

Rotation degree	Within_cluster sums							
	WS1	WS2	WS3	WS4	WS5	WS6	WS7	WS8
10	164	270	397	543	691	868	1114	1369
15	164	270	397	543	691	868	1114	1369
20	164	270	397	543	691	868	1114	1369
35	164	270	397	543	691	868	1114	1369
40	164	270	397	543	691	868	1114	1369
50	164	270	397	543	691	868	1114	1369
60	164	270	397	543	691	868	1114	1369
70	164	270	397	543	691	868	1114	1369
80	164	270	397	543	691	868	1114	1369
90	164	270	397	543	691	868	1114	1369
180	164	270	397	543	691	868	1114	1369
270	164	270	397	543	691	868	1114	1369



Table 8: WCS for fingerprint 1 with different resolutions

Resolution	Within_cluster sums							
	WS1	WS2	WS3	WS4	WS5	WS6	WS7	WS8
600x385 x1	164	270	397	543	691	868	1114	1369
1300x1009x3	164	270	397	543	691	868	1114	1369
368x267x1	164	270	397	543	691	868	1114	1369
265x190x1	164	270	397	543	691	868	1114	1369
283x178x1	164	270	397	543	691	868	1114	1369
500x355x3	164	270	397	543	691	868	1114	1369
1079x650x3	164	270	397	543	691	868	1114	1369
280x180x3	164	270	397	543	691	868	1114	1369