THE METHOD OF VICINITY MINUTIAE DECOMPOSITION WITH HIGHER LEVEL GRAPHS FOR FINGERPRINT VERIFICATION

The subject matter of the paper is the development of fingerprint local structures based on the new method of the minutia vicinity decomposition (MVD) for the solution to the task of fingerprint verification. It is an essential task because it is produced attempts to introduce biometric technology in different areas of social and state life: criminology, access control system, mobile device applications, banking. The goal is to develop real number vectors that can respond to criteria for biometric template protection schemes such as irreversibility with the corresponding accuracy of equal error rate (EER). The problem to be solved is the problem of accuracy in the case of verification because there are false minutiae, disappearing of truth minutiae and there are also linear and angular deformations. The method is the new method of MVD that used the level of graphs with many a point from 7 to 3. This scheme of decomposition is shown in this paper; such a variant of decomposition is never used in science articles. The following results were obtained: description of a new method for fingerprint verification. The new metric for creating vectors of real numbers were suggested – a minimal path for points in the graphs. Also, the algorithm for finding out minimal paths for points was proposed in the graphs because the classic algorithm has a problem in some cases with many points being 6. These problems are crossing and excluding arcs are in the path. The way of sorting out such problems was suggested and examples are given for several points are 20. Results of false rejection rate (FRR), false acceptance rate (FAR), EER are shown in the paper. In this paper, the level of EER is 33 % with full search. 78400 false and 1400 true tests were conducted. The method does not use such metrics as distances and angles, which are used in the classical method of MVD and will be used in future papers. This result is shown for total coincidences of real number, not a similarity that it is used at verifications. It is a good result in this case because the result from the method index-of-max is 40 %.

Keywords: fingerprint verification; minutia vicinity decomposition; false rejection rate; false acceptance rate; equal error rate; the minimal path for points in the graph.

Introduction

At present, there are attempts to introduce biometric technology for identification and verification in different informational protection services [1, 2], such as criminology, access control, and identification systems, e-commerce systems, general informational security systems (authorization and access to the information system), voting and electronic digital signature systems, electronic payments, state identification projects (border crossing, visas), etc. Fingerprint recognition is a problem that has been studied for 40 years and it is still an open issue.

It should be noted that despite huge number of published articles no one service (protocol) has been developed that used biometric data and responded all requirements of integrity, authenticity, accessibility, and information systems confidentiality and services [3, 4].

Minutia cylinder codes [5] are minutiae based fingerprint description that used 3D cylinder structures. Each cylinder is a local structure and contains data about spatial and directional contributions of minutia. It should be noted that this method is very hard for implementation. Vectors of real numbers is quite massive and the full process of verification can take 24 hours. This method has an advantage is high accuracy, EER might be 2…8 % for different data bases.

In the paper [6, 7] authors propose a ranking-based sensitive hashing for biometric protection that used so-called index-of max (IoM) for biometric fingerprint protection. This method IoM used cylinder structures [5], multiplication of matrixes, and choice by the maximum. This method is enough good for voice verification (EER 7 %), but results are not good enough for fingerprints. EER is about 40 %. The speed of verification after writing templates is quite high.

In [8] the authors proposed the method which is called MVD for obtaining a vector of real numbers. This method has advantages: simplicity and fast fingerprint verification. The method allows constructing local structures. Also, it provides stability to linear and angular deformations and resistance to appear false minutiae and disappear truth ones as in [5]. The scheme of decomposition is shown in Figures 1, 2. But this method also has a disadvantage - low accuracy. Figure 2 is shown the decomposition of the real fingerprint from a database.
Method MVD was criticized in the paper [9] because an attacker can create a fake fingerprint with a set of artificial minutia vicinity from the compromised template. Matcher simply can compare the features of minutiae triangles directly without knowledge of minutiae locations and orientations.

It is suggested binarization of vectors decreases the speed of verification. The task of binarization is solved in many papers like [5, 10]. But after using these methods the quality of vectors is decreased.

The MVD method with higher-level graphs solves all problems that were mentioned above: accuracy, time of verification, and the criteria of security. The goal of the research is to develop real number vectors that can respond to criteria for biometric template protection schemes such as irreversibility with the corresponding accuracy of equal error rate (EER).

1. Schema of MVD with higher level graphs

According to [11] minutia template is \( T=\{m_1, m_2, \ldots, m_n\} \). Each minutia is a triplet \( m=\{x_m, y_m, \theta_m\} \), where \( x_m \) and \( y_m \) is a minutia location or coordinate, \( \theta_m \) – is a minutia direction, \( n \) – amount of minutiae in template.

The paper suggests the method based on MVD [8], but it uses the higher level graphs. It is not possible to be completely sure about existence or absence of any minutia. For this reason in the paper proposed the new schema of decomposition for each minutia from template of fingerprint (Figure 3). The schema is described below with the real example. The method consists of local structures construction [5]. Local structures are the structures connected with local coordinate systems of each minutia.

In the Figure 4, a and Figure 4, b there is the vicinity that consists of 8 minutiae, these are the nearest minutiae. Coordinates of these minutiae are seeing in the Figure 4, b. The number of possible variants of decomposition can be calculated with using well known formula:

\[
C^k_n = \frac{n!}{k!(n-k)!},
\]

where \( n \) – amount of minutiae from vicinity;
\( k \) – amount of minutiae are supposed really exist in the vicinity.

According to (1) the number of possible decompositions is calculated in the Table 1. If the number of exist minutiae are 7 and 1 minutia is false, it might be 8 possible variants of decompositions.

The number of false minutiae can be 2, so the number of possible decompositions are 28. The total amount of variants are 218. Also the schema of decomposition is shown in the Figure 5.

| The number of vicinity minutiae | The number of probably true minutiae | The number of probably false minutiae | The number of combinations |
|---------------------------------|---------------------------------------|---------------------------------------|---------------------------|
| 8                               | 7                                     | 1                                     | 8                         |
| 8                               | 6                                     | 2                                     | 28                        |
| 8                               | 5                                     | 3                                     | 56                        |
| 8                               | 4                                     | 4                                     | 70                        |
| 8                               | 3                                     | 5                                     | 56                        |
|                                 |                                       | \( \Sigma \)                            | 218                       |

In the last case triangles are considered, there are 56 variants. Preparation of such variants is not a problem and has a solution to any amount of points.

In the Table 2 and 3 examples of these decompositions with coordinates that were chosen in the Figure 3 are shown. The variants with only one and two probably false minutiae were presented. As a result were obtained the graphs with number of point from 7 to 3. Some of these graphs are shown in the Figure 4.

For creating of these graphs was used basic well known algorithm finding shortest distance between points. This algorithm was described below in this paper with changes for providing absence of crossing arcs of graphs.

2. The basic algorithm to find out shortest distance between points

Properties of solution of salesman task such as resistance to points mixing, linear and angular transformations, were studied in [12]. These properties make it possible to use for biometric identification.

In this paper algorithm was used to sort out the salesman task [13]:

1. Preparation of matrix of mutual distances \( n \times n \).
2. Finding minimal values of distances in rows.
3. Subtraction minimal values of distances from corresponding rows.
4. Finding minimal values of distances in each column.
5. Subtraction minimal values of distances from corresponding columns.
6. As the result, a minimum one zero element has to be in each row and corresponding to each zero element there is the constant of bringing, this is the sum of minimal values in the corresponding row and column.
7. Choice of bringing constant with the biggest values.
8. Include the corresponding arc \( (i, j) \) in the path.
9. Exclude some arc from matrix by including the sign \( \infty \).
Fig. 1. Vicinity of minutia m, scheme of vicinity minutia decomposition

Fig. 2. Vicinity minutia decomposition on the real fingerprint according to [8]

| m1  | 8 variants of decomposition | 28 variants of decomposition | 56 variants of decomposition | 70 variants of decomposition | 56 variants of decomposition |
|-----|-----------------------------|-----------------------------|-------------------------------|-------------------------------|-------------------------------|
|    | Graphs with 7 true minutiae | Graphs with 6 true minutiae | Graphs with 5 true minutiae   | Graphs with 4 true minutiae   | Graphs with 3 true minutiae   |
| m2  | Graphs with 7 true minutiae | Graphs with 6 true minutiae | Graphs with 5 true minutiae   | Graphs with 4 true minutiae   | Graphs with 3 true minutiae   |
| mn  | Graphs with 7 true minutiae | Graphs with 6 true minutiae | Graphs with 5 true minutiae   | Graphs with 4 true minutiae   | Graphs with 3 true minutiae   |

Fig. 3. Vicinity minutiae decomposition according to the MVD with higher level graphs method
process. It was discussed in the [14] and shown examples in Tables 4.

10. Cross out i-row and j-column from the matrix.

11. Repeat 2-10 until the matrix has not size (n-2)(n-2).

12. The last two arcs are needed to choose from the elements, where the excluding is not put.

13. Looking throw the path to find out crossing arcs.

14. Deleting the crossing arcs by changing two points on the arcs, example of this was shown bellow (Table 5 and Figure 6) [14].

Table 2

| № | Possible variants of decompositions, one minutia is false | Path |
|---|--------------------------------------------------------|------|
| 0 | 0 1 2 3 4 5 6 | 274,3 |
| X | 115 149 103 102 173 158 104 |
| Y | 395 361 361 349 390 420 311 |
| 1 | 0 1 2 3 4 5 7 | 244,2 |
| X | 115 149 103 102 173 158, 157 |
| Y | 395 361 361 349 390 420 347 |
| 2 | 0 1 2 3 4 6 7 | 300,1 |
| X | 115 149 103 102 173 104 157 |
| Y | 395 361 361 349 390 311 437 |
| 3 | 0 1 2 3 5 6 7 | 289,5 |
| X | 115 149 103 102 158 104 157 |
| Y | 395 361 361 349 420 311 437 |
| 4 | 0 1 2 4 5 6 7 | 300,9 |
| X | 115 149 103 173 158 104 157 |
| Y | 395 361 361 390 420 311 437 |
| 5 | 0 1 3 4 5 6 7 | 307,2 |
| X | 115 149 102 173 158 104 157 |
| Y | 395 361 349 390 420 311 437 |
| 6 | 0 2 3 4 5 6 7 | 301 |
| X | 115 103 102 173 158 104 157 |
| Y | 395 361 349 390 420 311 437 |
| 7 | 1 2 3 4 5 6 7 | 302,3 |
| X | 149 103 102 173 158 104 157 |
| Y | 361 361 349 390 420 311 437 |

Table 3

| № | Possible variants of decompositions, two minutiae are false | Path |
|---|---------------------------------------------------------|------|
| 0 | 0 1 2 3 4 5 | 217,5 |
| X | 115 149 103 102 173 158 |
| Y | 395 361 361 349 390 420 |
| 1 | 0 1 2 3 4 6 | 249,3 |
| X | 115 149 103 102 173 104 |
| Y | 395 361 361 349 390 311 |
| 2 | 0 1 2 3 4 7 | 243,3 |
| X | 115 149 103 102 173 157 |
| Y | 395 361 361 349 390 437 |
| 3 | 0 1 2 3 5 6 | 262,8 |
| X | 115 149 103 102 158 104 |
| Y | 395 361 361 349 420 311 |
| 4 | 0 1 2 3 5 7 | 232,7 |
| X | 115 149 103 102 158 157 |
| Y | 395 361 361 349 420 437 |
| 5 | 0 1 2 3 4 5 6 7 | 297,3 |
| X | 149 102 173 158 104 157 |
| Y | 361 349 390 420 311 437 |
| 7 | 2 3 4 5 6 7 | 298,8 |
| X | 103 102 173 158 104 157 |
| Y | 361 349 390 420 311 437 |

Table 4

| Iteration number | Arcs from path | Arcs for excluding |
|------------------|----------------|--------------------|
| 0                | 14; 15         | 15; 14             |
| 1                | 16; 18         | 18; 16             |
| 2                | 3; 11          | 11; 3              |
| 3                | 11; 5          | 3; 5               |
| 4                | 4; 6           | 6; 4               |
| 5                | 6; 16          | 4; 18              |
3. Results of experiments

In this research each minutia is represented by the vector. The amount of the closest minutiae is 10 was used for creating feature vectors. The size of the vectors was n*56, where n – the number of minutiae in templates. Restriction on the radius of vicinity is up to 60.

78400 false and 1400 true tests were carried out with using database from [15]. Each template in database is represented by p1_p2, where the first number p1 is the number of person; the second number p2 is the position of the finger. For example, all numbers of coincidence were given in the Table 6 for both 0_0 and 0_1 templates.

Fig. 5. Graphic representations of some variants of decompositions from Tables 2 and 3:

- a – all minutiae are true, graph with 8 points;
- b – one minutia with coordinates (157, 437) is false, graph with 7 points;
- c – one minutia with coordinates (104,311) is false, graph with 7 points;
- d – one minutia with coordinates (158,420) is false, graph with 7 points;
- e – two minutiae with coordinates (103,361) and (115,395) are false, graph with 6 points, 26th variants from Table 3;
- f – two minutiae with coordinates (149,361) and (115,395) are false, graph with 6 points, 27th variants from Table 3.
The results for true and false experiments are shown in the Table 5.

| Point from the path | X' | Y' | X'' | Y'' | X''' | Y''' | X'''' | Y'''' |
|---------------------|----|----|-----|-----|------|------|-------|-------|
| 0                   | 111| 173| 111| 173| 111| 173| 111| 173 |
| 1                   | 115| 151| 115| 151| 151| 151| 151| 151 |
| 2                   | 151| 182| 151| 182| 151| 182| 151| 182 |
| 3                   | 168| 201| 168| 201| 168| 201| 168| 201 |
| 4                   | 171| 214| 171| 214| 171| 214| 171| 214 |
| 5                   | 196| 216| 196| 216| 196| 216| 196| 216 |
| 6                   | 214| 229| 214| 229| 214| 229| 214| 229 |
| 7                   | 225| 247| 225| 247| 225| 247| 225| 247 |
| 8                   | 221| 252| 221| 252| 221| 252| 221| 252 |
| 9                   | 216| 263| 216| 263| 216| 263| 216| 263 |
| 10                  | 101| 368| 137| 380| 137| 380| 137| 380 |
| 11                  | 115| 392| 115| 392| 115| 392| 115| 392 |
| 12                  | 137| 380| 101| 368| 101| 368| 101| 368 |
| 13                  | 166| 231| 166| 231| 176| 240| 148| 129 |
| 14                  | 176| 240| 176| 240| 166| 231| 166| 231 |
| 15                  | 148| 248| 148| 248| 148| 248| 176| 240 |
| 16                  | 159| 281| 159| 281| 159| 281| 159| 281 |
| 17                  | 129| 308| 129| 308| 129| 308| 129| 308 |
| 18                  | 108| 267| 108| 267| 108| 267| 108| 267 |
| 19                  | 111| 173| 111| 173| 111| 173| 111| 173 |

Fig. 6. Excluding crossing arcs from the optimal solution:
a – solution X', Y'; b – the fifth iteration of deleting crossing arcs X''', Y''''.

Table 6

| Total amount of numbers is 272 for experiment 0_0 and 0_1 |
|----------------------------------------------------------|
| 354; 299; 349; 231; 314; 262; 394; 325; 328; 368; 306; 317; 343; 373; 373; 352; 352; 448; 284; 371; 308; 371; 288; 243; 303; 220; 263; 194; 194; 279; 302; 216; 303; 237; 325; 319; 285; 375; 319; 323; 250; 295; 312; 314; 218; 381; 296; 286; 270; 325; 271; 238; 287; 287; 314; 266; 336; 301; 255; 375; 375; 378; 378; 316; 254; 327; 333; 299; 237; 231; 305; 253; 350; 326; 324; 225; 314; 291; 338; 264; 299; 288; 270; 287; 282; 282; 347; 369; 337; 313; 310; 352; 353; 357; 320; 297; 280; 325; 311; 253; 271; 324; 404; 306; 228; 263; 310; 351; 315; 315; 234; 234; 370; 322; 234; 296; 331; 365; 351; 337; 303; 341; 346; 365; 260; 322; 301; 242; 335; 254; 345; 302; 327; 302; 387; 282; 314; 277; 273; 340; 273; 293; 293; 350; 385; 221; 301; 396; 263; 324; 318; 330; 401; 330; 343; 286; 286; 328; 240; 381; 369; 292; 292; 292; 250; 375; 271; 196; 242; 276 |

There are 272 coincidences as also it is shown in the Table 6. Comparisons of existing methods of verifications are shown in the Table 7. Also some other results for true and false experiments are shown in Table 8. Considering the experiment 0_0 and 0_1, the result is 272 coincidences as in Table 8. In the Figure 7 FAR, FRR and EER are presented. EER is 33 %.
Table 7

Comparisons of existing methods of verifications

| Method                  | Reference  | Time for template writing | Time for full verification | EER, % | Algorithm for verification |
|------------------------|------------|---------------------------|---------------------------|--------|---------------------------|
| MCC                    | [5]        | 37 minutes                | 24 hours                  | 2-8 %  | Based on similarity       |
| MCC+IOM                | [5, 6, 7]  | 37+15 minutes             | 1 hour                    | 40 %   | Full coincidences         |
| MVD                    | [8, 7]     | 17 minutes                | 35 minutes                | 23 %   | Based on similarity, vulnerability according [7] |
| MVD with higher level graphs | Our paper | 1 hours                   | 30 minutes                | 33 %   | Full coincidences         |

To decrease EER the future research will use vectors which consist of features as in [8]:

\[ u_r = (s_1, r, \Delta \alpha_1, \alpha_1 r_1, s_2, \Delta \alpha_2, \alpha_2 r_2, s_3, \Delta \alpha_3, \alpha_3 r_3) \] (2)

where \( s_1, s_2, s_3 \) denote the length of the three side of a triangle; \( r=1, \ldots, 4 \) corresponding to Figure 1; \( \alpha_1, \alpha_2, \alpha_3 \) – represent the internal angles; \( \alpha_1 r_1, \alpha_2 r_2, \alpha_3 r_3 \) are the orientations for minutiae of the triangle. First results of addition verification are shown in the Table 9, 10, Figure 8, a and Figure 8, b. This research was carried out on the templates 0_0 and 0_1 from [15].

Table 8

Values of number for full coincidences in the templates

| Values of metric for false tests | Values of metric for true tests |
|---------------------------------|--------------------------------|
| 92                              | 172                            |
| 77                              | 176                            |
| 113                             | 246                            |
| 146                             | 262                            |
| 135                             | 253                            |
| 190                             | 282                            |
| 151                             | 267                            |
| 96                              | 210                            |
| 140                             | 222                            |
| 86                              | 200                            |
| 112                             | 202                            |
| 125                             | 201                            |

Conclusions

In the research the solution for verification task of fingerprint was suggested. Our solution has advantages (Table 7):

- high speed of extracting the vectors of real values, because of changing the algorithm of finding minimal distances,
- high speed of matching templates of real vectors in compare with cylinder codes in [9].

The solution has disadvantages such as low accuracy for some tests, but it can be improved by adding features, such as angles and distances of which consist our graphs [8]. And it has to be noticed that in such program finding parameters and testing are required a huge amount of time. EER=33 %. This result is not as good as in [5], but matching of templates was carried out for total coincidences of real number, not a similarity that is used at verifications. This is better result than in [6], because the result from the method index-of-max is 40 %.

Fig. 7. FRR pink and red curves, FAR – blue curve, EER =33%: a – full chart; b - enlarged part of chart
Table 9

| №  | Path  | \( s_i \) |
|-----|-------|-----------|
| 0_0 | 222   | 51 45 33 32 29 15 14 |
| 0_1 | 220   | 51 45 34 32 28 16 12 |

Table 10

| X    | Y    | X    | Y    |
|------|------|------|------|
| 177  | 435  | 186  | 415  |
| 163  | 409  | 173  | 390  |
| 193  | 395  | 205  | 377  |
| 206  | 388  | 221  | 374  |
| 215  | 400  | 228  | 384  |
| 247  | 402  | 260  | 389  |
| 221  | 447  | 229  | 430  |
| 177  | 435  | 186  | 415  |

Fig. 8. Demonstration of addition verification for the future research; red color for the template 0_0 and blue color for the template 0_1:

- a – full chart;
- b – enlarged part of chart

References (GOST 7.1:2006)

1. Mathematical model of the biometric system of fingerprint authentication [Text] / Serghii Rassomakhin, Kate Budianska, Anna Uvarova, Mykhaylo Bagmut // Комп’ютерні науки та кібербезпека. – 2019. – № 1(13) – С. 4–16. DOI: 10.26565/2519-2310-2019-1.01.

2. Efficient fuzzy extraction of puf-induced secrets: theory and applications [Text] / Jeroen Delvaux, Dawy Ga, Ingrid Verbauwhede et al. // Conference: International Conference on Cryptographic Hardware and Embedded Systems – CHES 2016. – 2016. – Vol. 9813. – P. 412–431. DOI: 10.1007/978-3-662-53140-2_20.

3. Мигаль, Г. В. Коллектив та ергономічні аспекти взаємодії людини з комп’ютером [Текст] / Г. В. Мигаль, В. П. Мигаль // Радіоелектронні і комп’ютерні системи. – 2020. – № 1. – С. 90–102. DOI: 10.32620/reks.2020.1.09.

4. Wawrzynski, T. Artificial intelligence and curbculture [Текст] / Tomasz Wawrzynski // Радіоелектронні і комп’ютерні системи. – 2020. – №3(95). – С. 20–26. DOI: 10.32620/reks.2020.3.02.

5. Minutia texture cylinder codes for fingerprint matching [Text] / Wajih Ullah Baig, Umar Munir, Waqas Ellahi, Adeel Ejaz, Kashif Sardar // 2019 International Conference on Frontiers of Information Technology (FIT), 2019. – P. 1–12. DOI: 10.1109/FIT47737.2019.00024.

6. Ranking based locality sensitive hashing enabled cancelable biometrics: index-of-max hashing [Text] / Zhe Jin, Jung Yeon Hwang, Yen-Lung Lai, Soohyang Kim, Andrew Beng Jin Teoh // IEEE Transactions on Information Forensics and Security. – 2018. – Vol. 13, Iss. 2. – P. 393–407. DOI: 10.1109/TIFS.2017.2753172.

7. Cryptographic Key Generation from PUF Data Using Efficient Fuzzy [Text] / H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura // Conference: The 16th International Conference on Advanced Communications Technology (ICACT2014), IEEE Xplore, 2014. – P. 23–26. DOI: 10.1109/ICACT.2014.6778915.

8. Zhe, A. J. Fingerprint template protection with Minutia Vicinity Decomposition [Text] / Andrew Jin Zhe, Andrew Teoh Beng Jin // 2011 International Joint Conference on Biometrics (IJCB), 2011. – P. 1–7. DOI: 10.1109/IJCB.2011.6117597.

9. Non-invertible graph-based hamming embedding transform for fingerprint protection [Text] / Zhe Jin, Bok-Min Goi, Andrew Beng Jin Teoh, Yong Haur Tay // 2014 International Conference on Electronics, Information and Communications (ICEIC),
2014. – P. 1-2. DOI: 10.1109/ELINFOCOM.2014.6914439.

10. Multi-Bit Allocation: Preparing Voice Biometrics for Template Protection [Text] / H. M. Paulini, C. Rathgeb, A. Nautsch, H. Reichau, H. Reininger, C. Busch // Conference: Speaker and Language Recognition Workshop (Odyssey 2016). – Bilbao, Spain, 2016. – P. 291-296. DOI: 10.21437/Odyssey.2016-42.

11. ISO/IEC 19794-2:2005. Information technology – biometric data interchange formats – Part 2: Finger minutiae data [Text]. – International organization for standardization ISO Central Secretariat, 2005. – 40 p.

12. Мелкоzerosa, O. М. Ідентифікація отпечатків пальців на основі гамильтонових циклів розподілу локальних признаків [Текст] / О. М. Мелкоzerosa, С. Г. Рассомахін // Вісник Харківського національного університету імені В. Н. Каразіна. Серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління : сб. наук. пр. – Харків, 2019. – Том. 44. – С. 51–65. DOI: 10.26565/2304-6201-2019-44-06.

13. Taha, Hamdy A. Operations Research: An Introduction [Text] / Hamdy A. Taha. – 10th edition. – Pearson Education Limited, 2017. – 843 s.

14. Мелкоzerosa, O. Верифікація відбитків пальців з використанням рішення задачі комівожжера і декомпозиції оточення мініцій [Текст] / О. Мелкоzerosa, С. Малков, В. Гайкова // Комп’ютерні науки та кібербезпека. – 2020. – № 2(18). – С. 25–32. DOI: 10.26565/2519-2310-2020-2-03.

15. Fingerprint data base [Electronic resource]. – Access mode: http://www.fingerprint-it.com/wp-content/uploads/2017/03/CrossMatch_Sample_DB.zip - 28.09.2021.

References (BSI)

1. Rassomakhin, S., Budyans’ka, K., Uvarova, A., Bahmut, M. Mathematical model of the biometric system of fingerprint authentication. Kompu’terni nauky ta kiberbezpeka – Computer science and cybersecurity, 2019, no. 1(13), pp. 4–16. DOI: 10.26565/2519-2310-2019-1-01.

2. Delvaux, J., Gu, D., Verbauwhede, I. et al. Efficient fuzzy extraction of puf-induced secrets: theory and applications. Conference: International Conference on Cryptographic Hardware and Embedded Systems – CHES 2016, vol. 9813, pp. 412-431. DOI: 10.1007/978-3-662-53140-2_20.

3. Myhal, H. V., Myhal, V. P. Kohnityvni ta erhonomichni aspekty vzayemodiyi lyudyny z kompu’ternom [Cognitive and ergonomic aspects human interaction with a computer]. Radioelektronnyi i kompu’terni sistemi – Radioelectronic and computer systems, 2020, no. 1, pp. 90-102. DOI: 10.32620/reks.2020.1.09.

4. Wawrzynski, Tomasz. Artificial intelligence and cuberculture. Radioelektronnyi i kompu’terni sistemi – Radioelectronic and computer systems, 2020, no. 3(95), pp. 20-26. DOI: 10.32620/reks.2020.3.02.

5. Baig, Wahjih Ullah, Munir, Umar., Ellahi, Waqas., Ejaz, Adeel., Sardar, Kashif. Minutia texture cylinder codes for fingerprint matching. 2019 International Conference on Frontiers of Information Technology (FIT), 2019, pp. 1-12. DOI: 10.1109/ FIT47737.2019.00024.

6. Jin, Zhe., Hwang, Jung Yeon., Lai, Yan-Lung. et al. Ranking based locality sensitive hashing enabled cancelable biometrics: index-of-max hashing. IEEE Transactions on Information Forensics and Security, 2018, vol. 13, iss. 2, pp. 393-407. DOI: 10.1109/TIFS.2017.2753172.

7. Kang, H., Hori, Y., Katashita, T., Hagiwara, M., and Iwamura, K. Cryptographic Key Generation from PUF Data Using Efficient Fuzzy. Conference: The 16th International Conference on Advanced Communications Technology (ICACT2014), IEEE Xplore, 2014, pp. 23-26. DOI: 10.1109/ICACT.2014.6778915.

8. Zhe, A. J., Jin, A. T. B. Fingerprint template protection with Minutia Vicinity Decomposition. 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1-7. DOI: 10.1109/IJCB.2011.6117597.

9. Jin, Zhe., Goi, Bok-Min., Jin, Allongg Bendo. Teoh., Tay, Yong Haur. Non-invertible graph-based hamming embedding transform for fingerprint protection. 2014 International Conference on Electronics, Information and Communications (ICEIC), 2014, pp. 1-2. DOI: 10.1109/ELINFOCOM.2014.6914439.

10. Paulini, H. M., Rathgeb, C., Nautsch, A., Reichau, H., Reininger, H., Busch, C. Multi-Bit Allocation: Preparing Voice Biometrics for Template Protection. Conference: Speaker and Language Recognition Workshop (Odyssey 2016), Bilbao, Spain, 2016, pp. 291-296. DOI: 10.21437/Odyssey.2016-42.

11. ISO/IEC 19794-2:2005. Information technology – biometric data interchange formats – Part 2: Finger minutiae data. International organization for standardization ISO Central Secretariat, 2005. 40 p.

12. Мелкоzerosa, O. M., Rassomakhin, S. G. Ідентифікація отпечатків пальців на основі гамильтонових циклів розподілу локальних признаків [Идентификация отпечатков пальцев на основе гамильтоновых циклов распределения местных признаков]. Bulletin of V.N. Karazin Kharkiv National University, series «Mathematical modeling. Information technology.»
МЕТОД ДЕКОМПОЗИЦІЇ ОКОЛИЦЬ МІНУЦІЙ З ВИКОРИСТАННЯМ ГРАФІВ БІЛЬШОГО ПОРЯДКУ ДЛЯ ВЕРИФІКАЦІЇ ВІДБІТКІВ ПАЛЬЦІВ

С. Г. Рассомахін, О. М. Мелкозьорова, О. П. Нарежний

Предметом навчання статті – розробка локальних структур відбитків пальців, який засновується на методі декомпозиції околиць мінуцій для вирішення задачі верифікації відбитків пальців. Це дуже важлива задача, тому що призводяться спроби введення біометричних технологій у різні області соціального та державного життя. Мета полягає у розробці відбитків пальців для вирішення задачі верифікації відбитків пальців.

Внутрішня задача состоит в вирішенні задачи верифікації відбитків пальців. Це дуже важлива задача, тому що призводяться спроби введення біометричних технологій у різні області соціального та державного життя.

Мета полягає у розробці відбитків пальців для вирішення задачі верифікації відбитків пальців. Це дуже важлива задача, тому що призводяться спроби введення біометричних технологій у різні області соціального та державного життя.

Предметом навчання статті – розробка локальних структур відбитків пальців, який засновується на методі декомпозиції околиць мінуцій для вирішення задачі верифікації відбитків пальців. Це дуже важлива задача, тому що призводяться спроби введення біометричних технологій у різні області соціального та державного життя.
получены следующие результаты: описание нового метода для верификации отпечатков пальцев. Мы предложили новую метрику для построения векторов - минимальное расстояние между точками в графах. В статье также приведены усовершенствованный алгоритм для поиска минимального расстояния, так как классический алгоритм имеет проблемы в некоторых случаях с количеством точек от 6. Эти проблемы: это дуги, которые пересекаются и исключения дуг из маршрута. Мы предложили путь решения этой проблемы и привели пример с количеством точек, равным 20. Результаты уровня ложного отказа (FRR), уровня ложного доступа (FAR), эквивалентная ошибка (EER) показаны в статье. Мы провели 78400 ложных и 1400 действительных испытаний. Можно сформулировать следующие выводы: уровень EER равен 33 % при полном переборе при тестировании. Это не лучшие результаты в мире, но при наполнении векторов действительных чисел мы не использовали расстояния между минуциями и углы, которые используются в классическом методе MVD. В последующих исследованиях мы будем использовать эти метрики дополнительно. Также надо обозначить, что результаты приведены для полного совпадения чисел, а не для сходства векторов, как это применяется при верификации. Это довольно неплохой результат, потому что результат при применении метода по максимальному индексу составляет около 40 %.

**Ключевые слова:** верификация отпечатков пальцев; декомпозиция окрестностей минуций; уровень ложного отказа; уровень ложного доступа; уровень эквивалентной ошибки; минимальное расстояние в графе.

**Рассомахин Сергій Геннадійович** – д-р техн. наук, зав. каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

**Мелкольумова Ольга Михайлівна** – канд. техн. наук, доц. каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

**Нарежний Олексій Павлович** – канд. техн. наук, доц. каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

**Sergiy Rassomakhin** – PhD, doctor of technical science, professor, head of department of information systems and technologies security V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, e-mail: rassomakhin@karazin.ua, ORCID: 0000-0003-1394-3588, Scopus Author ID: 6602387161.

**Olha Melkozerova** – PhD, associate professor of department of information systems and technologies security V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, e-mail: olha.melkozerova@karazin.ua, ORCID: 0000-0002-1134-2925.

**Oleksii Nariezhnii** – PhD, associate professor of department of information systems and technologies security V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, e-mail: o.nariezhnii@karazin.ua, ORCID: 0000-0003-4321-0510, Scopus Author ID: 57201777102.