International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

# A Non-Invertible Cancellable Fingerprint Template for Low-Quality Fingerprints

**Likhit J Jain[1], Abhiram Sridhar Puranam[2], Ken Jonathan Pais[3], Mamatha K R[4]**

*[1,2,3]Student, Department of Information Science and Engineering, BMS College of Engineering, Bangalore, India.*
*[4]Assistant Professor, Department of Information Science and Engineering, BMS College of Engineering, Bangalore, India.*

---

**Abstract -** *Non-invertible cancellable biometrics are a combination of the ease of biometric identification and cryptographic security. An effective method to solve the issue of fingerprint security are fingerprint templates. In this study, we create a robust and accurate cancellable fingerprint template, which works with low-quality fingerprint images. We utilize Delaunay's Triangulation Net to produce a 3-dimensional array from the minute points retrieved from the fingerprint. The user key is generated by passing a hex string that gets converted into a 3x4 matrix. These two features produce a cancellable template of the fingerprint. This template is used as a high secure authentication template in biometrics systems. The cancellable template satisfies the requirements of revocability, unlikability, non-invertibility and performance.*

***Key Words***: Biometrics, Fingerprint Recognition, Cancellable Fingerprint, Delaunay Triangulation Net, Minutiae Points, Non-Invertibility, Revocability, Template Security

## 1. INTRODUCTION

Biometrics are physical or behavioural human traits that are digitally used to identify a person. They are unique to each individual, and to enhance accuracy, they can be used in combination with traditional identification systems. Some examples of these biometric identifiers are fingerprints, iris, voice, DNA. As long as the following requirements are satisfied, any human trait may be utilised as a biometric: [1]:

- Universality: The biometric characteristic must be present on all subjects;
- Distinctiveness: The biometric characteristic must be distinct for any two given subjects;
- Permanence: The biometric characteristic must be stable and not vary over time;
- Collectability: The biometric characteristic must be easily acquired and must have the ability to be measured quantitatively.

If the above requirements are satisfied, biometrics can be used for authentication in a wide array of environments. Biometric Systems are pattern recognition systems that gather a person's biometrical information, derives a feature set from obtained information and compares it to a template set in the database [2]. A realistic biometric system should be used to satisfy precision, speed and resource requirements, which are non-hazardous for users and are approved by intended users. There is a need for biometric robustness even in low-quality fingerprints. We use a cancellable template as a solution for this problem. The storing of a modified version of a biometric template is necessary for cancellable biometrics and hence provides more privacy, enabling the linking of numerous templates with biometric data that is equal [3]. This helps to ensure that biometric data is unlinkable. A cancellable template must satisfy the following qualities [4]:

- Revocability: The transformed template must have the ability to be revokable and reissuance with a new template must be possible using the same user's biometric data;
- Unlinkability: It must not be possible to link two templates of the same user. Also, the same cancellable template must not be used across various biometric systems. The two transformed templates must look independent of each other.
- Non-invertibility: Obtaining the original template from a modified template must be computationally challenging.
- Performance: When compared with performance without transformation, biometric recognition utilising template transformation must be efficient.

Cancellable fingerprint templates are of two types: (i) Registration Based; or (ii) Alignment-free. Registration-based methods require that singular points be accurately detected. [5]. However, in this method, any errors will produce a false reject (Type – I error) and thus a faulty cancellable template [6]. Furthermore, any absence of singular points will increase the False Rejection Rate (FRR) and affect subsequent processing [7]. In alignment-free or registration-free methods, both, global and local features of minutiae point on the fingerprint are considered for transformation [8].

## 2. RELATED WORD

A cancellable fingerprint template's key concept is not to save the original fingerprint template since this safeguard's users' data. Fingerprints are irreplaceable and number-bound in the human body. The permanent loss of the data subject will lead to any security compromise in the fingerprint database. Therefore, many converted templates of the same fingerprint are maintained and offer additional levels of anonymity, using a modified fingerprint template. It

also helps to promote a broad range of apps' non-linkability of user fingerprints.

Fingerprints have demonstrated a tremendous capacity to replace the standard password system or token safety. The encryption of a biometric fingerprint using a hash feature is a straightforward technique. To get its original fingerprint model, it is very hard to reverse engineering processed template. This fulfils the non-invertibility characteristic and is a significant element to safeguard sensitive information. One disadvantage is that even minute changes in the input can generate significantly different results. Fingerprints may readily be influenced by the surroundings in the actual world. Slight changes in illumination or sweat on the fingers can make a large variation in the fingerprint template.

Many templates have been sought to solve this restriction. Yang et al. [9] have examined 8 distinct kinds of fingerprint attacks. Ratha et al. have analyzed the weaknesses of the present system [10]. According to them, the template database along with its sensor module are the most vulnerable to attacks. They also offered the first technique of solving a cancellable biometric template. Cancellable biometrics alter the novel template in such a manner that the possibility to calculate the novel template from the modified one is not there. An alignment-free fingerprint cancellable template using minutia templates has been proposed by Ahn et al [11]. Ahmad et al employed rotational-free and translation-less polar co-ordinates for information between tiny locations rather of employing Cartesian co-ordinates [12]. A Minutia Cylinder-Code (MCC) based cancellable fingerprint template has been developed Ferrara et al. [13-15]. The use of a cancellable fingerprint biometric template might increase identification accuracy and template security, according to Yang et al [9], and proposed a cancellable fingerprint template formed zoned minutia pair [16]. A structure based on Delaunay's Triangulation was used by Yang et. al to calculate cancellable fingerprint template [17]. A cancellable fingerprint template is proposed by Sandhya et. al based-on Delaunay triangular structure [18]. Delaunay triangulation for indexing fingerprint template database was put to use by Khodadoust et al [19].

The minute topological features may be represented with computer geometric techniques easily and effectively. Delaunay triangulation and Voronoi diagram are two approaches extensively utilized in biometric fingerprint alignment or local alignment of the minutiae. For structural stability under random positional noise, Tüceryan et. al. carried out a thorough comparison research [20]. Delaunay triangulation has been shown to be less susceptible to noise. The triangulation of points in Delaunay has also been proven to be stable under random disruption of positions by Bebis et al[21]. The arrangement of the minutia points varies across impressions that have the same fingerprint template, however what remains same is their topological structure. The number of detailed elements in different impressions of the same fingerprint likewise varies. These fluctuations may be handled extremely competently by the Delaunay triangulation of minute points. In the fingerprint templates as Soleymani et al showed, the Voronoi diagram is likewise highly successful in alignment but the template they offer is not free of alignment [22]. Our technique presented offers an earlier solution and meets the cancellable and non-invertible fingerprint template criteria.

## 3. PROPOSED METHOD

The core idea of our cancellable fingerprint template which we have suggested is to produce 4-dimensional matrix utilizing minute triangles. The 4-dimentional matrices are then utilized for user authentication as a fingerprint template. The following stages are provided in the proposed framework:

i. Construction of Delaunay Triangulation Net from minutiae
ii. Feature extraction
iii. Computation of 4-Dimentional Feature Set and Generation of Cancellable template
iv. Fingerprint Matching

The flow chart for the proposed method is depicted in figure 1.

### 3.1. Construction of Delaunay Triangulation Net from minutiae

Minutiae points $m_i = (x_i, y_i, \theta_i)^n{}_{i=1}$ is extracted, the number of minutiae is represented by 'n', in the fingerprint. The coordinates of the minutiae and its orientation are represented by '$(x_i, y_i)$', '$\theta_i$', respectively. A Voronoi diagram is created from the minutiae points which separates the whole region into miniscule divisions. A minutia point $m_i$ is just one in every tiny location. Then, by linking the thoroughness of each area with its neighbouring regions, Delaunay Triangulation Net is created [23]. Structurally, Delaunay's Triangulation has more stability. This is the rationale for adopting Delaunay's method of triangulation. If a fingerprint image has a variable distortion, each detail has the same structure as the minute details beneath the tolerance zone [24].

### 3.2. Feature Extraction

For the feature extraction in the Delaunay triangulation net, the interior angles of each triangle were used. The main steps are as follows:

i. A triangle $\triangle m_1m_2m_3$ is selected from Delaunay triangulation net.

ii. Directions $d_i$ ($i$ = 1, 2, 3) of the vectors from the centroid of the triangle to each vertex $m_i$ ($i$ = 1, 2, 3) are computed.

iii. The interior angle $\alpha_i$ ($i$ = 1, 2, 3) between the normalized vectors from each minutia to the remaining minutiae is calculated.

iv. Interior angles $(\alpha_1, \alpha_2, \alpha_3)$ calculated in the previous step are aligned and sorted in ascending order of $d_i$.

v. The above procedure is repeated for each and every triangle in the fingerprint.

Figure 2(a) shows the fingerprint with the minutiae and figure 2(b) shows the same fingerprint image with Delaunay's Triangulation Net plotted.

### 3.3. Computation of 4-Dimentional Feature Set and Generation of Cancellable Template

With the user-specific key, a 3-dimensional matrix set of features is projected in 4-dimensional space. Applications that allow 4-dimensional templates to be diverse, are set differently. The user-specific key is chosen by passing a hexstring, that gets converted to a 3x4 matrix. Multiplying the 3-dimensional characteristics set with the user-specific key yields the projected 4-dimensional matrix which is the required features set.

### 3.4. Fingerprint Matching

Two templates are taken for the proposed matching method and its similarity score calculated. For a template to match, two templates $T_1$ and $T_2$ are taken. An attempt is made by the matching algorithm to search for the most optimal match for feature vector, $t_1$ from $T_1$ among the other feature vectors, $t_2$ of $T_2$. A comparison is then made between feature vector $t_1$ from $T_1$ and each and every feature vector, $t_{2j}$ from $T_2$. A possible match is regarded if and only if the distance between the feature vectors is less than the given tolerance τ. The most optimal match which is the feature vector with minimal distance from among all the available matches, is selected. The similarity value 'S' is computed using Equation 1 on the basis of the total number of the match and the mismatch count.

$$S(T_1,T_2) = \frac{(match_{count} - mismatch_{count})}{(\frac{length(T_1) + length(T_2)}{2})}$$

Algorithm 1 provides the proposed template matching algorithm.

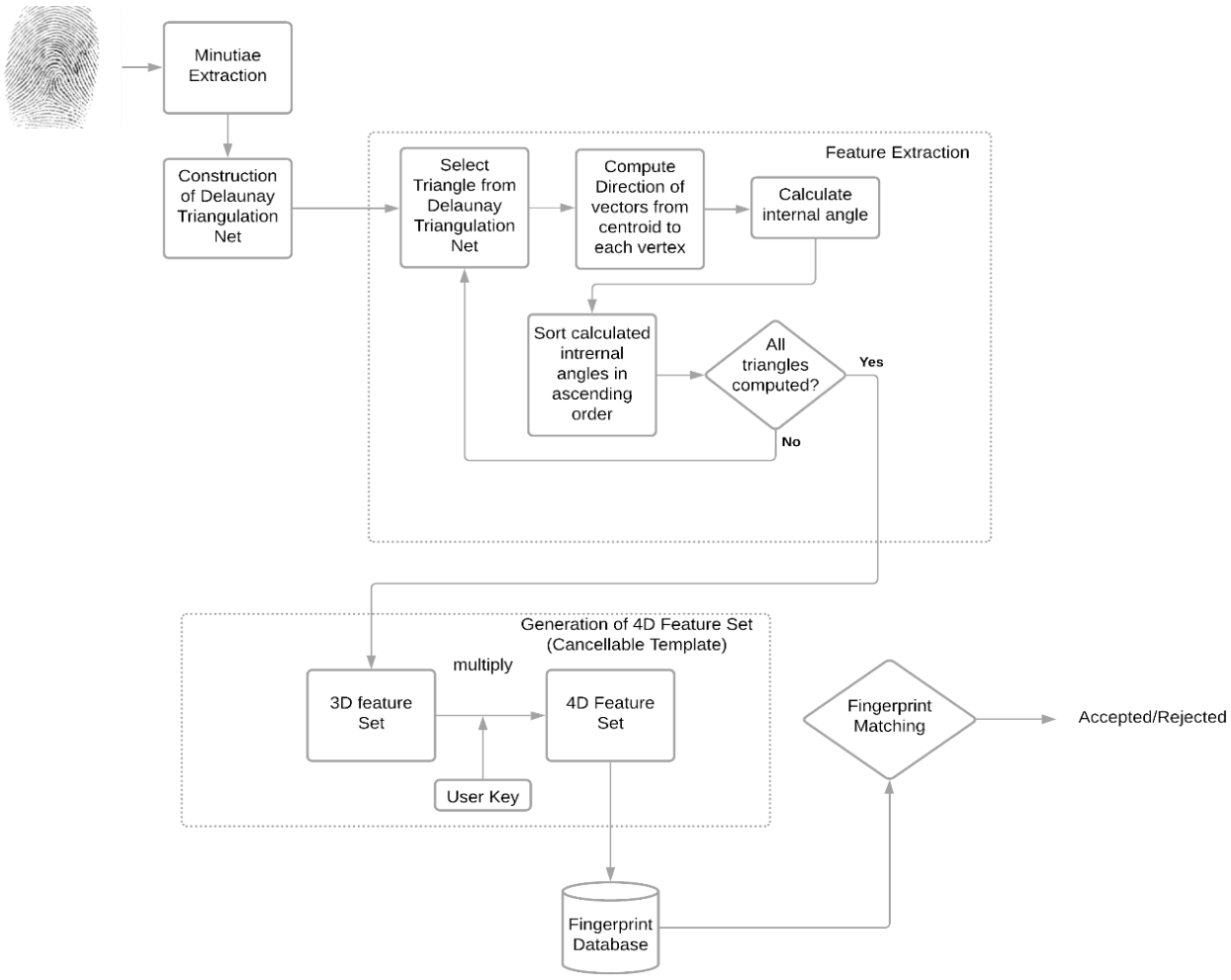


*Figure 1: Flowchart of Proposed Framework*

*Algorithm 1: Proposed Template Matching algorithm*

***Input:*** *Two fingerprint templates '$T_1$',' $T_2$',and threshold 't'*
***Output:*** *Similarity Score 'S'*

***procedure*** *MATCHING ($T_1$, $T_2$, t)*
***For*** *$t_1$ in $T_1$* ***Do***

```
    d ← d_MAX
    k ← 0
    For t2 in T2 Do
        t1.sort()
        t2.sort()
        dist ← distance.euclidean(t1, t2)
            If dist <= t and dist <= d Then
                d ← dist
                match_count ← matchcount + 1
                enrolled_template.remove(t2)
            Else
                mismatch_count ← mismatch_count + 1
            Endif
            k ← k + 1
    Endfor
  Endfor
return S ←(match_count-mismatch_count))/(((length(T_1 )+length(T_2))/2))
endProcedure
```

## 4. EXPERIMENTAL SETUP

Fingerprint databases FVC 2002 DB1, DB2, DB3 and FVC 2004 DB1, DB2, DB3 are used to test our proposed methods [25, 26]. Details of FVC 2002 and FVC 2004 databases are in Table 1.

| Database | | Sensor | Image | Resolution |
|---|---|---|---|---|
| **FVC 2002** | **DB1** | Optical | 388x374 | 500 dpi |
| | **DB2** | Optical | 296x560 | 569 dpi |
| | **DB3** | Capacitive | 300x300 | 500 dpi |
| **FVC 2004** | **DB1** | Optical | 640x480 | 500 dpi |
| | **DB2** | Optical | 328x364 | 500 dpi |
| | **DB3** | Thermal | 300x480 | 512 dpi |

*Table 1: Information on FVC 2002 and FVC 2004 Databases*

## 5. PERFORMANCE METRICS

The performance measures considered in our experiment are false acceptance rate (FAR), false rejection rate (FRR), genuine acceptance rate (GAR), genuine rejection rate (GRR) and equal error rate (EER). The false acceptance rate (FAR) is the measure of the probability that an unauthorised user is mistakenly trying to enter the biometric security system. The FRR is a measure of the probability of an access attempt made by an authorised user via the biometric security system being rejected erroneously. The probability of FAR and FRR being equal is EER. GAR is the ratio of the number of inputs to the total number of positive input samples is properly classifiable and GRR is the ratio of the number of input samples successfully identified as an imposter to the total number of impostor input samples.

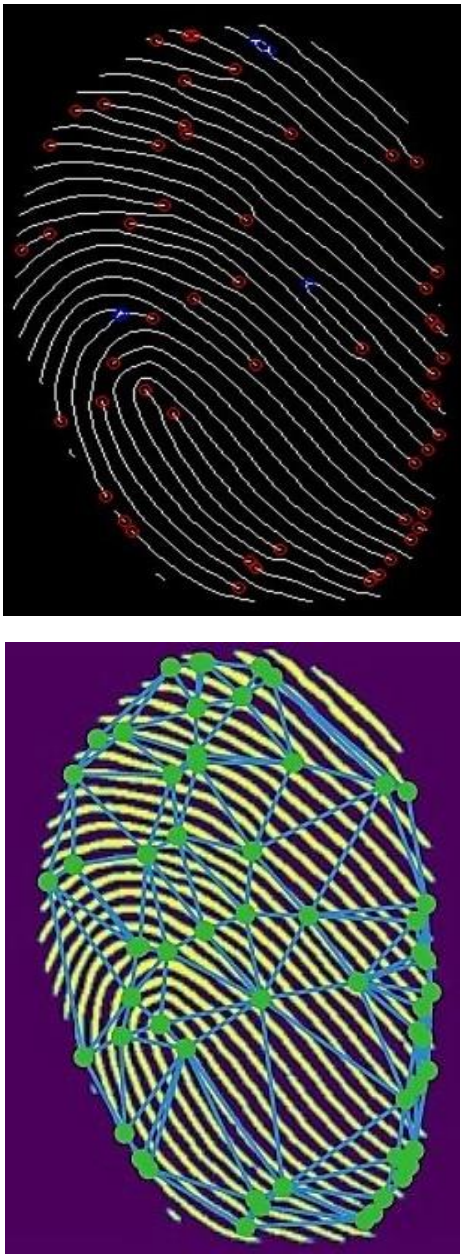

*Figure 2: (a) Fingerprint image with minutiae (b) Delaunay Triangles on the same fingerprint image.*

## 6. RESULTS AND DISCUSSIONS

We compared our proposed method with other similar existing methods of fingerprint template protection in terms of EER. The comparison is shown in Table 2.

### 6.1 Comparison with other models

| EER | FVC 2002 | | | FVC 2004 | | |
|---|---|---|---|---|---|---|
| | DB | DB | DB | DB1 | DB2 | DB3 |
| Trivedi et. al [34] | 1.2 | 2.1 | - | - | - | - |
| Ahmad et al. [28] | 9 | 6 | 27 | - | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| Das et al. [29] | 2.27 | 3.79 | - | - | - | - |
| Wang and Hu [8] | 3.5 | 4 | 7.5 | - | - | - |
| Jin et al. [31] | 5.19 | - | - | 15.76 | 11.64 | - |
| Yang et al. [30] | 3.36 | 0.59 | 9.8 | 16.51 | 14.88 | - |
| Yang et al. [16] | 5.93 | 4 | - | - | - | - |
| Jin et al. [32] | 4.36 | 1.77 | - | 24.71 | 21.82 | - |
| Sandhya et al. [18] | 3.96 | 2.98 | 6.89 | 12.17 | 13.29 | 17.7 |
| Lee et al. [33] | 1.82 | 1.06 | 2.2 | 2.46 | - | - |
| **Proposed** | **1.0** | **0.7** | **1.5** | **2.34** | **3.13** | **4.68** |

### 6.2 Unlinkability

Two distinct templates from the same fingerprint should not be well matched in order to make the fingerprint recognition systems a legitimate mark of a single fingerprint. To assess unlinkability, we randomly chose two different user keys for two biometric systems. Each fingerprint template was compared with another template of the same subject. The two systems showed high degree of unlinkability. This shows that the proposed template satisfies the condition of unlinkability.

### 6.3 Revocability

Biometric revocability means the generation, if necessary, of a new template from the same biometric sample. If a fingerprint template is compromised by an attacker, a second fingerprint template may be generated from the same fingerprint picture, the template and method for the template manufacture are considered as being revisable. A new template may then be produced with a different user key set of the same fingerprint picture, corresponding to a leaked User Template, if there is a template data base assault and the template is released. If a user template is likely to be harmed or stolen by our suggested method, a new template may be created with a newer user key and the same fingerprints image without the worry that the promised com template is detected by the attacker. If a new template with a new user key and the same fingerprint photo are likely to be stolen or impacted, the enemy can be created without the enemy being recognized through a promised com template. The prior template with the attacker does not fit the new template authentically and there can be no attack. The new templates and old templates are divided and the template can be abolished.

### 6.4 Security

Non-invertibility of cancellable templates assures that the computational construction of the original biometrics from the changed template is not possible. Sandhya et al. assume that the security analysis scenario is attacked by the adversary attacks [18]. They constructed a feature set using the Delaunay triangle on three sides. There are neighboring triangles in the Delaunay triangulation network. The neighboring triangles therefore are of the same length with respect to a side line. Finally, the Delaunay Triangulation Net consisting of tiny points may be recreated using the feature set. The approximate location of fingerprints is therefore clear.

## 7. CONCLUSION

A fingerprint biometric technology that generates a cancellable template was researched to address several drawbacks of the conventional token or password authentication method. In this paper, we presented a cancellable fingerprint template based on the Delaunay triangulation net. Our method works exceptionally well for low-quality fingerprints. On the fingerprint image, detailed minutiae points are located and extracted. Then, the cancellable template is generated using Delaunay's Triangulation Net and the user-key which is a hexstring. The FVC 2002 and FVC 2004 database was used to test the performance of the proposed template. The EER results demonstrate high efficiency for the suggested template. Concerns of security and privacy were addressed and one of these problems is the safety of user templates. The study of the experiment reveals the strength of the technology concerning revocability, unlinkability, non-invertibility and performance.

## REFERENCES

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics, Springer Science & Business Media, New York, NY, USA, 2011.

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), 4-20.

[3] Teoh, A. B., Kuan, Y. W., & Lee, S. (2008). Cancellable biometrics and annotations on biohash. Pattern recognition, 41(6), 2034-2044.

[4] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on advances in signal processing, 2008, 1-17.

[5] Nalini K. Ratha, Sharat Chikkerur, Jonathan Connell, and Ruud Bolle. Generating cancelable fingerprint templates. IEEE Transaction on PAMI, April 2008.

[6] Chikkerur, S., Ratha, N. K., Connell, J. H., & Bolle, R. M. (2008, September). Generating registration-free cancelable fingerprint templates. In 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems (pp. 1-6). IEEE.

[7] Wang, S., & Hu, J. (2013, December). A Hadamard transform-based method for the design of cancellable fingerprint templates. In 2013 6th International

Congress on Image and Signal Processing (CISP) (Vol. 3, pp. 1682-1687). IEEE.

[8] Wang, S., Hu, J.: 'Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach', Pattern Recogn., 2012, 45, pp. 4129–4137

[9] Yang, W. , Wang, S. , Hu, J. , Zheng, G. , Valli, C. , 2019. Security and accuracy of finger- print-based biometrics: a review. Symmetry 11 (2), 141.

[10] Ratha, N.K. , Connell, J.H. , Bolle, R.M. , 2001. Enhancing security and privacy in bio-metrics-based authentication systems. IBM Syst. J. 40 (3), 614–634.

[11] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8, IEEE, Darmstadt, Germany, 2014.

[12] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, "Matching with secure fingerprint templates using non-invertible transform," in Proceedings of the 2008 Congress on Image and Signal Processing, vol. 2, pp. 29–33, IEEE, Sanya, China, May 2008.

[13] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1727–1737, 2012.

[14] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8, IEEE, Darmstadt, Germany, 2014.

[15] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: a new representation and matching technique for fingerprint recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 12, pp. 2128–2141, 2010.

[16] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," Pattern Recognition, vol. 66, pp. 295–301, 2017.

[17] Yang, W., Hu, J., Wang, S., Yang, J., 2013. Cancelable fingerprint templates with delaunay triangle-based local structures. In: Cyberspace Safety and Security. Springer, pp. 81–91.

[18] Sandhya, M., Prasad, M.V.N.K., Chillarige, R.R., 2016. Generating cancellable fingerprint templates based on delaunay triangle feature set construction. IET Biomet. 5 (2), 131–139. doi:10.1049/iet-bmt.2015.0034.

[19] Khodadoust, J., Khodadoust, A.M., 2017. Fingerprint indexing based on expanded delaunay triangulation. Expert Syst. Appl. 81, 251–267.

[20] Tüceryan, M., & Chorzempa, T. (1991). Relative sensitivity of a family of closest-point graphs in computer vision applications. Pattern Recognition, 24(5), 361-373.

[21] Bebis, G., Deaconu, T., Georgiopoulos, M., 1999. Fingerprint identification using delaunay triangulation. In: International Conference on Information Intelligence and Systems. IEEE, pp. 452–459.

[22] Soleymani, R., Amirani, M.C., 2012. A hybrid fingerprint matching algorithm using Delaunay triangulation and Voronoi diagram. In: 0th Iranian Conference on Electrical Engineering (ICEE), 2. IEEE, pp. 752–757.

[23] S. Fortune, "Voronoi diagrams and delaunay triangulations," in Handbook of Discrete and Computational Geometry, J. E. Goodman and J.O'Rourke, Eds., pp. 377–388, CRC Press, Inc., Boca Raton, FL, USA, 1997.

[24] M.Abellanas, F.Hurtado, andP.A. Ramos, "Structural tolerance and delaunay triangulation," Information Processing Letters, vol. 71, no. 5-6, pp. 221–227, 1999.

[25] Fingerprint Verification Competition 2002: http://bias.csr.unibo.it/fvc2002/databases.asp

[26] Fingerprint Verification Competition 2004: http://bias.csr.unibo.it/fvc2004/databases.asp

[27] Neurotechnology, Verifinger SDK, http://www.neurotechnology.com.

[28] Ahmad, T., Hu, J., Wang, S.: 'Pair-polar coordinate-based cancelable fingerprint templates', Pattern Recogition, 2011, 44, pp. 2555–2564

[29] Das, P., Karthik, K., Garai, B.C.: 'A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs', Pattern Recogn., 2012, 45, pp. 3373–3388

[30] Yang, W., Hu, J., Wang, S., et al.: 'An alignment-free finger-print bio-cryptosystem based on modified Voronoi neighbor structures', Pattern Recogn., 2014, 47, pp. 1309–1320

[31] Jin, Z., Teoh, A.B.J., Ong, T.S., et al.: 'Fingerprint template protection with minutiae-based bit-string for security and privacy preserving', Expert Syst. Appl., 2012, 39, pp. 6157–6167

[32] Jin, Z., Lim, M.-H., Teoh, A.B.J., et al.: 'A non-invertible randomized graph-based hamming embedding for generating cancelable finger-print template', Pattern Recogn. Lett., 2014, 42, pp. 137–147

[33] Lee, S., & Jeong, I. R. (2019). A cancelable template for the low-quality fingerprints from wearable devices. Security and Communication Networks, 2019.

[34] Trivedi, A. K., Thounaojam, D. M., & Pal, S. (2020). Non-Invertible cancellable fingerprint template for fingerprint biometric. Computers & Security, 90, 101690.