A Novel Security Of Biometric Cryptosystems And Transformation For Fingerprint Template Protection

Priyanshu Pandey
School of Computing Science and Engineering
, Galgotias University, Uttar Pradesh, India.
E-mail: priyanshupandey006@gmail.com

Himanshu Negi
School of Computing Science and Engineering
, Galgotias University, Uttar Pradesh, India.
E-mail: himanshu.negi8786@gmail.com

C.Remesh
School of Computing Science and Engineering
, Galgotias University, Uttar Pradesh, India.
E-mail: c.remesh@galgotiasuniversity.edu.in

Abstract— With a fingerprint distinguishing framework, templates are put away in the server database. To keep away from the protection concerns on the off chance that the database is bargained, numerous methodologies of securing biometrics templates, for example, biometric encryption, salting, and noninvertible transformation are proposing to upgrade security. Nonetheless, a single methodology may not meet all application prerequisites, including security, diversity, and revocability. In this paper, we show a hybrid plan for securing fingerprint templates, which coordinates our novel calculations of biometric encryption and noninvertible transformation. This plan can give high security, diversity, and revocability. Test results demonstrate the near execution of those approaches.

Index Terms— bio-encryption, hybrid, protection, salting, template

1 INTRODUCTION

Biometrics delivers an unquestionable confirmation of individual character offering more security and comfort than customary strategies for individual distinguishment. On the other hand, clients still have a few concerns: Such privacy issues should be unraveled. Layout security is a privacy- enhancing measure in the use of biometrics. It is broadly acknowledged that in an immaculate plan of layout security, templates must be applied independently, concealable, secure, what's more, have good performance of coordinating. Scientists propose some successful methodologies, for example, salting, noninvertible transformation, and key era from biometrics cryptosystems, be that as a singlemethodology may not be sufficiently secure.

A single methodology is not sufficient to meet all necessities. Salting gives high diversity, revocability, what's more precision, yet its invertible transformation can't meet

The security necessity, particularly, in the event that the key or the layout is lost. Noninvertible transformation can give more security over-salting yet the security-precision issue exists. Biometric encryption is viewed as the most guaranteeing innovation yet plans of which may, in any case, have some helplessness. In this paper, we propose a hybrid plan for securing fingerprint templates, brushing biometric encryption with noninvertible transformation, which is more secure than any single methodology [1]. The next section deals

with the related work and section III deals with the proposed architecture followed by experiments and results. A comparison chart is also given with few metrics and finally, the paper ends with a conclusion.

2 RELATED WORK

The Methods for protecting biometric templates can be divided into two categories, namely feature conversion (reversible biological data) and biometric cryptosystem.

2.1 Fuzzy Vault Systems

Fuzzy vault systems do not store the original template in the database. Instead, a changed adaptation of the layout is put away just with the assistance of cryptography. In [1], a brief description of these biometric cryptosystems, their issues, and challenges are given. A brief introduction of the fuzzy system is given by [2]. The helper data inclusion was proposed by J.P. Linnartz [3] and this is a modification made to [2] by finding a higher degree polynomial to the template which will only take the minutiae points from the genuine set. With the help of the work that is already scheming, Wang [4] presented an implementation work of the paper by Sujitha et al

[2] using some helper data [5] and showed how this helper data is helping to prevent the information leakage.

Descriptions are made relative to [2]. Herrera [6] prepared the way for a suitable algorithm that solved two problems: the calculation of relevance and similarity. The purpose of blurred engagement systems is to protect biometrics by encrypting polynomial estimates. The descriptors, add some modifications to this methodology for greater security. Fingerprint registration or alignment is essential to reduce fluctuations within the class in the unencrypted domain to calculate alignment parameters. In general, bio cryptosystems fall into two categories, namely, adjustment and non-adjustment-based methods [7]. In the basement of the method of Juels ([8], [9]), Jan et al.

[19] developed a new system for solving single deviation points and small point changes using local Voronoi neighboring structures based on the bio cryptosystem without adjusting to fixed-length bitmaps.

2.2 Cancellable Biometrics

Cancellable biometrics alludes to the efficiently repeatable bending of biometric includes so as to ensure touchy client explicit information. On the off chance that a cancellable component is undermined, the bending qualities are changed, and similar biometrics are mapped to another layout, which is utilized hence [10]. The techniques by and large fall into two classifications: (I) Biometric Salting and (ii) Non-invertible Transforms.

K. Simoens [11] gave an insight into the weaknesses of privacy, asking "whether a person could endanger the privacy of a user accessing biometric encrypted documents" and examining "whether an attacker could determine two documents in the same biometric encryption. "In doing so, they set the conditions for the perfect differentiation of the enemy's benefits and their perfect irreversibility.

Y. Sutcu et al. [12] proposed a one-way transformation method in combination with cryptographic security. hash functioning fact, it is designed as a combination of various Gaussian functions to function as "healthy hash". The cryptographic hash is used to protect biometric templates stored in the database. The algorithm with the ORL face database and showed that this system offers a valuable solution to one of the weaknesses of privacy and security of templates.

So far, the algorithms that were proposed using the cancellable domain still have some demerits. That is, they either avoid the distribution of biometric features or used an inefficient feature matching which leads to security threats. Hence, Nagar et.al [20] proposed a system for non- invertible fingerprint template transformation which takes the “coverage effort curve” into account for measuring the number of guesses required by an adversary to find some portion of biometric identity. Another set of work deals with minutiae-based transforms under cancellable template protection. Chen, H. et al [13] gave a pragmatic work in which transform does not depend on the application so that templates cannot be reused.

There are many methods available to protect biometric templates, but it is not easy to create a method that meets the criteria set by Teoh, Goh and Ngo [14]: (i) diversity (ii) reversibility (iii) irreversibility and (iv) effectiveness after analyzing, Z. Jin et al. al [7] presented a method for creating a fingerprint recovery pattern relative to a bit fiber using a three-way polarization quantization technique. Fingerprint mosaics lead to the reconciliation of information obtained from two or more fingerprints by combining these impressions into a single mosaic, or by combining characteristics (ie details) of such impressions as follows:

Jawline et. al [16] proposed a calculation that intertwined numerous biometric information at the elementary level to acquire an incorporated format to make sure about the melded layouts utilizing a crossover format assurance strategy. Layout security should be possible utilizing the data got from the local connection that is anticipated in a plane to produce a string which is then encoded utilizing a client's critical. In [17], their commitment is the development of M square shapes and multiline neighboring connection age.

They proposed an arrangement free cancellable layout age by developing M square shapes with various directions around each reference details followed by the figuring of revolution invariant and interpretation invariant neighboring connection, plane based quantization for bit string age and cancellable format age is finished with the assistance of neighbor particulars found in the M square shapes to create the multiline neighboring connection for each minutia in the unique mark.. But some prior methods use only some minutiae whose distance are greater than the threshold that is selected for template generation and after that, the matching process begins. The proposed method fulfills the necessary and sufficient conditions which are the primary requirements of a cancellable template design like non-inevitability, accuracy, diversity, and revocability.

3 PROPOSED SYSTEM ARCHITECTURE

In this approach, two strategies (that we have seen as of now in Section 2) are consolidated at two stages with extra changes in the current methods. Enlistment is to enroll a hybrid fingerprint template security using biometric encryption also noninvertible change. On the client-side, the customer checks his/her finger and gives C-Key and R-Key. On the other side, the structure first unites C-Key with exceptional finger impression particulars in the midst of biometric encryption and subsequently applies the noninvertible change to the fleecy points of interest with R-Key. The hybrid fingerprint template will be secured in the database.

3.1 Enrollment Phase

C-Key is bound to extract original minutiae from the fingerprint. C-Key is some private key or password to be protected. We construct a multivariable linear equation,the coefficients of which are determined by C-Key. C-Key is divided into m sub-keys, from which coefficients are generated one by one. (The entire enrolment process is given as Fig.1 (FP – fingerprint, DB – database used).

C-key <=> (ck1,ck2,… ckn) (1)

With the help of the above key, a polynomial equation is built and the solution for that is added to every minutia which is shown below.

ck1p1 + ck2p2+....+cknpn = b (2)

{(s1,mp1),(s2,mp2),...(sNT.mpNT)} (3)

where s1,s2, . . . sNT are the solutions to the equation and p1, p2 . . . pNT are the co-efficient of those parts of the equation. The combination of these two values will give rise to C-Key.

After these duplicate points (rdup) at the radial, angle θdup are added to the original minutiae(r) which is at the radial angle θ to spare the exact locations of minutiae focuses which holds the parts of the arrangements of the polynomial equation. In order to evade the overlapping of duplicate focuses on real minutiae that are having an arrangement part, we need to place them with respect to the reference minutiae just when the threshold is less than altered consistent worth. Here threshold refers to the greatest separation between two similar focuses.

$$|rdup-r| > threshold(r) \quad (4)$$

$$|\Theta dup-\Theta| > threshold(\Theta) \quad (5)$$

If two points satisfy either (4) or (5) we can place the duplicate point in the coordinate. Then, the regional transformation has to be done. Our noninvertible transformation is described as below: (1) A circular region is built around every minutia and represented a set of minutiae inside. The radius of regions is identical, but the number of minutiae changes from region to region. (2) Regional transformation. It is a process of transforming the minutiae region by region.

Suppose a region is represented as Reg (r, θ, α), then transform (Reg(r, θ, α), R-Key) = Reg (t1, t2) by

$$\begin{matrix} rk11, rk12, rk13 \\ rk21, rk22, rk23 \end{matrix} \quad \begin{matrix} r \\ \Theta \end{matrix} \quad \begin{matrix} t1X \\ t2 \end{matrix} \quad = \quad (6)$$

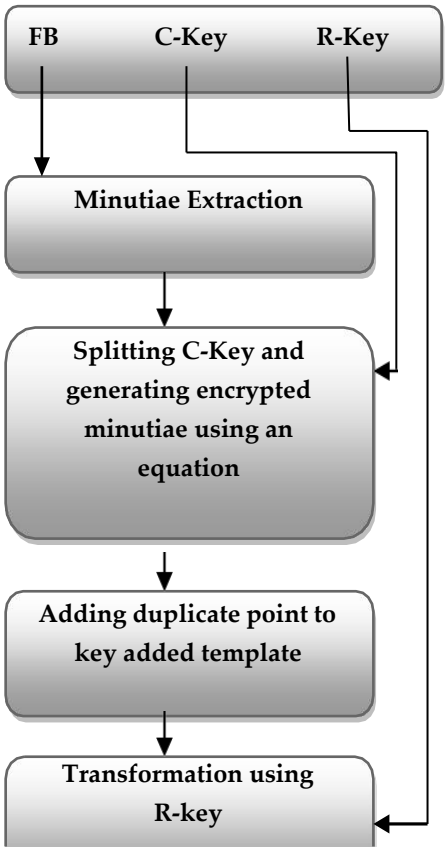

Fig.1: Enrollment Phase

3.2 Verification Phase

Recognition means the performing matching in the transformed form and C-Key generation from the hybrid template. When a user scans his/her finger and provides R-Key. Then the system first applies the noninvertible transformation to the input minutiae with R-Key and performs the matching in the transformed form. If the matching is successful, the system will find solutions of the linear equation, which are associated with matching minutiae, recover the original equation, and generate C-Key.

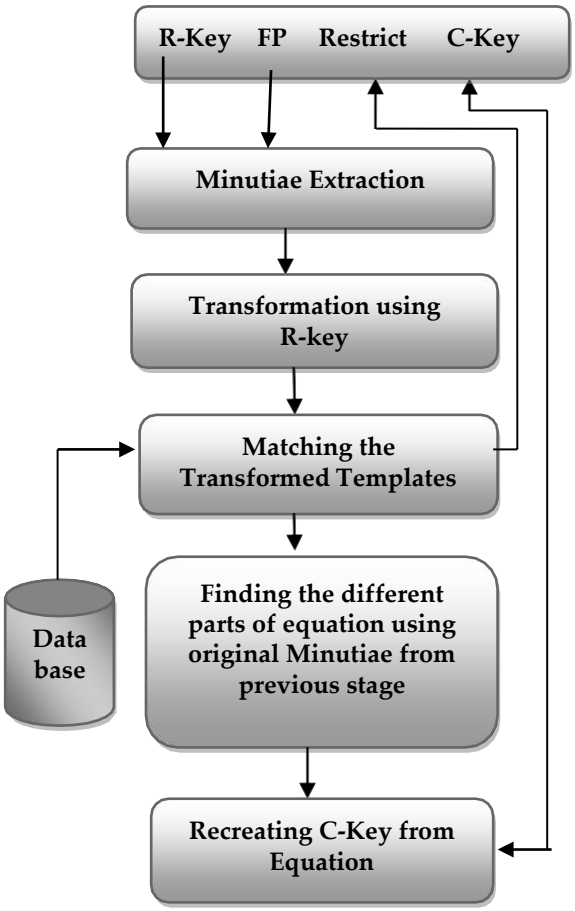

Fig.2: Verification Phase

In our scheme, the system performs matching in the transformed space region by region. Let (t1, t2) be a minutia of Reg (t1, t2), which is a transformed region from the input fingerprint, (tem1, tem2) be a minutia of Reg (tem1, tem2), which is a transformed region from the template, (tem1, tem2) and (t1, t2) are matched only if

$|t1\text{-}term1| \leq threshold(t1)$

$|t2\text{-}term2| \leq threshold(t2)$ (7)

Reg (t1, t2) and Reg (tem1, tem2) are matched regions only if the number of matched points reaches a threshold (Reg_match). Fig 2 (FP- fingerprint, DB – database used) explains the verification process. In this way both the template protection methods are used to encrypt the template and duplication is added to confuse the hacker while finding the key and only when the correct minutiae collection is found out, then there is a match.compared with the other algorithms available in the literature as shown in table I. It shows the evaluation of different template protection methods (that we have seen so far) along with the performance metrics like FAR (False Acceptance Rate), FRR (False Rejection Rate), GAR (Genuine Acceptance Rate), and EER (Equal Error Rate). Almost all methods endeavors to have less EER but it could not.

The evaluation results show that the methods applied to one application are comparatively producing lesser performance. Among these vulnerabilities, an attack against stored biometric templates is a real concern because of the solid linkage. The proposed algorithm along with its metrics is also given and the rise confidence about applying this algorithm is clearly shown

TABLE -1

EVALUATION OF VARIOUS FINGERPRINT TEMPLATE PROTECTION METHODS

Proposed BY	Methodology Used	Database Used	Success rate (GAR)	Success rate (FAR) /(FRR)	Error rate (EER)
Ting Wang. et al (2019) [4]	Fuzzy Fingerprint Vault, Constructing Helper Data	ICP based Alignment. DB2 database of FVC, 2016	72.6%	0% FAR	
Wencheng. et al (2018) [22]	Helper Data Extraction, Authentication	FVC2002 DB2.	95% (degree of 6)	0.01%	
Yang, W., Hu, J.,Wang, S., and Stojmenovic, M.(2014) [19]	Formation of VNSs, Generation of modified VNSs, Generation of fixed-length bit-string representations, Encrypted matching	FVC2000DB1, all of the 4 databases) of FVC 2002, and FVC2004DB2.			14.30% 11.84% 10.38% 16.52% 15.63% 20.61%
Machado et al (2018). [20]	Minutiae template transforms, non-invertibility measures.	FVC2002	92%	10%	
Chen, H., and Chen, H. (2017) [13]	Construct circular regions, Encrypt circular regions, Matching using encrypted regions	FVC2002 DB1 and DB2.	96.5% , 98.5% @ num level 18.	2% - DB1 2% - DB2 @ num level 18. (FAR)	
Ali et al (2015). [21]	(PGTQ): Reference minutia based polar transform, tuple-based quantization. Bit-string generation and User-specific tokenized permutation, Matching.	FVC2002 DB1& DB2 FVC2004 DB1& DB2.			1.19% 6.94% 16.35% 8.66%
Chin, Y. J. Ong, T. S.et al (2014) [16]	Feature level fusion, Random tiling, Feature Discretization.	2 fp & 2 palm print databases.			
Prasad, M. V. N. K., and Santhosh C. (2014). [17]	Multiline neighboring relation generation, Plane based quantization and bitstring generation, Cancellable template generation, Matching.	FVC 2002 DB1, DB2 and DB3.	FVC 2002 DB1, DB2 and DB3.		0.62% 1.33% 2.64%
Proposed Hybrid Algorithm	Minutiae Extraction, Splitting Key, Adding Duplicate points, R-Key Transformation, Matching, C-Key Generation	DB	98%	0 to 2 %	

4 IMPLEMENTATION AND RESULTS

A fuzzy vault, noninvertible transformation and hybrid scheme are explored. Experiments are conducted on FVC2002 that consists of 140 images (388 X 374 dimensions). For each approach of securing fingerprint templates, a new template is first constructed for each instance of each finger and then matching is performed between the template and other instances of the same finger. Fingerprint matching is also performed in the original form [18]. Figure 3 shows the accuracy of different approaches. In our noninvertible transformation, the transformation example, do not differentiate among departments of the same organization). Transforms the three-dimension space of (r, θ, β) into a two-dimension space of (h1, h2), which makes the template less discriminating but more robust against brute-force attacks. In our hybrid scheme, both chaff points are generated and noninvertible transformation is performed to the fingerprint template, which makes the template more "noisy". The complexity against brute force attacks can reach 412 bits in case only the transformed template is compromised.

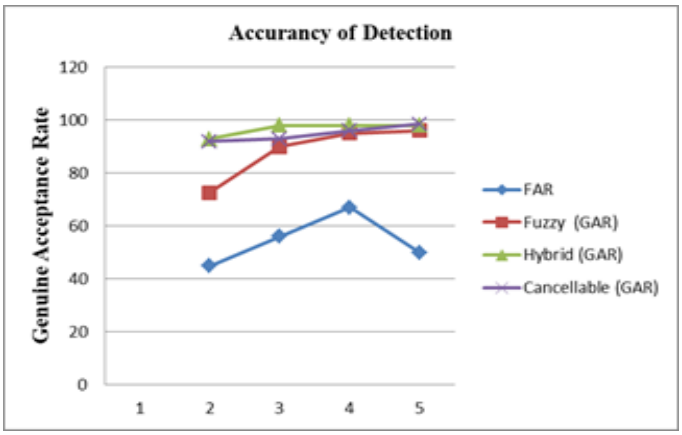

Figure 3: Evaluation of basic & hybrid Approaches

The above graph shows the GAR and FAR for the basic approaches like fuzzy and featured transformation techniques applied individually on the fingerprint data set. Finally, the combined approach for fingerprint template protection technique which was applied to the same data set is given in the graph. The data set used for this graph is given in table 2. It explains that the FAR increases as the data set increases but GAR never decreases after saturation level. Hybrid Approach gives the FAR of 2 only at a very large set of data. The rest gives at the earlier stage of increasing data count. So this algorithm can be applied for some databases with more instances of single fingerprint and yet minimum FAR can be achieved.

TABLE 2

DATA SET FOR THE ABOVE GRAPH

FAR	*Fuzzy*	*Hybrid*	*Cancellable*
	(GAR)	*(GAR)*	*(GAR)*
0	*72.6*	*93*	*92*
0.5	*90*	*98*	*93*
1.5	*95*	*98*	*96*
2	*96*	*98*	*98.5*

5 CONCLUSION

A hybrid plan has been introduced for securing fingerprint templates, which consolidates biometric encryption with noninvertible transformation. In our hybrid plan, a fuzzy vault utilizing a linear equation and chaff points is connected to the original fingerprint layout, to begin with, then a noninvertible transformation changes all details points' area by the district. Just the double transformed structure is put away in the disjoin database. Contrasted with the two fundamental methodologies, the hybrid plan is more robust against brute-force assaults, which implies the format of our plan is harder to be traded off. Also, our novel methodology can also give high diversity of what's more revocable. Essentially, a "new" fingerprint layout can be issued by essentially evolving PIN. In any case, because of the chaff points and noninvertible transformation, the layout is less segregating, which makes the coordinating precision drop a smidgen.

REFERENCES

1. Yang, Wencheng, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. "Security and accuracy of fingerprint-based biometrics: A review." Symmetry 11, no. 2 (2019): 141.
2. Sujitha, V., and D. Chitra. "A Novel Technique for Multi Biometric Cryptosystem Using Fuzzy Vault." Journal of medical systems 43, no. 5 (2019): 112.
3. J. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," pp. 393–402, 2018. K. Elissa, "Title of paper if known," unpublished.
4. You, Lin, and Ting Wang. "A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion." Soft Computing23,no. 11 (2019): 3843-3851.
5. Chitra, D., and V. Sujitha. "Security analysis of prealigned fingerprint template using fuzzy vault scheme." Cluster Computing (2018): 1-9.
6. Romero, Luis F., Siham Tabik, Andrés Jesús Sánchez, Miguel Angel Medina Pérez, and Francisco Herrera. "A first step to accelerating fingerprint matching based on deformable minutiae clustering." (2018).
7. Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacypreserving," Expert Syst. Appl., vol. 39, no. 6, pp. 6157–6167, May 2012.
8. Chauhan, Sonam, and Ajay Sharma. "Improved fuzzy commitment scheme." International Journal of Information Technology (2019): 1-11. A. Juels and M. Sudan, "A Fuzzy Vault Scheme," Des. Codes Cryptogr.,vol. 38, no. 2, pp. 237–257, Feb. 2006.
9. Jin, Andrew TeohBeng, and Lim MengHui. "Cancelable biometrics."Scholarpedia 5.1 (2010): 9201.
10. K. Simoens, P. Tuyls, and B. Preneel, "Privacy Weaknesses inBiometric Sketches," 2009 30th IEEE Symp.Secur. Priv., pp. 188–203, May 2009.
11. Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric Multimedia authentication scheme based on robust hashing," Proc.7th Work. Secure. - MM&Sec '05, p. 111, 2005.
12. H. Chen and H. Chen, "A novel algorithm of fingerprint encryptionusing minutiae-based transformation," Pattern Recognit. Lett., vol. 32, no. 2, pp. 305–309, Jan. 2011.
13. A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispacequantization as an analytic mechanism for BioHashing ofbiometricand random identity inputs.," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 1892–901, Dec. 2017.
14. A. Ross, S. Shah, and J. Shah, "Image versus feature mosaicing : A case study in fingerprints," no. April, 2006.
15. Y. J. Chin, T. S. Ong, a. B. J. Teoh, and K. O. M. Goh, "Integratedbiometrics template protection technique based on fingerprint and palmprint feature level fusion, Inf-fusion ,vol - 18, pp- 161-174, Jul 2014.
16. M. V. N. K. Prasad and C. Santhosh Kumar, "Fingerprint templateprotection using multiline neighboring relation," Expert Syst. Appl., vol. 41, no. 14, pp. 6114–6122, Oct. 2014.
17. Chen, H. Sun, H., Lam, K.-Y, "A fast and elastic fingerprintmatching algorithm using minutiae-centered circular regions" In:Proceedings of International Conference on Emerging SecurityInformation, Systems, and Technologies, SecureWare 2007,pp. 211–215.
18. W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoineighbour structures," Pattern Recognition., vol. 47, no. 3, pp. 1309– 1320, Mar. 2014.
19. A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms" Abhishek Nagar and Anil K . Jain ∗
    Department of Computer Science and Engineering Michigan State University," pp. 81–85, 2009.
20. Machado, Sweedle, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar, and Priya Chaudhari. "Securing ATM Pins and Passwords Using Fingerprint Based Fuzzy Vault System." In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-6. IEEE, 2018.
21. Ali, Syed Sadaf, Iyyakutti Iyappan Ganapathi, and Surya Prakash. "Robust technique for fingerprint template protection." IET Biometrics 7, no. 6 (2018): 536-549.
22. Yang, Wencheng, Jiankun Hu, Song Wang, and Qianhong Wu. "Biometrics based privacy-preserving authentication and mobile template protection." Wireless Communications and Mobile Computing 2018 (2018).