Gmail **N P <nishkalprakash@gmail.com>**

ACM Transactions on Privacy and Security - Decision on Manuscript ID TOPS-2022-07-0137

ACM Transactions on Privacy and Security <onbehalfof@manuscriptcentral.com> 3 November 2022 at 17:40
Reply-To: ninghui@purdue.edu
To: fagulpandey@gmail.com, priya.fav67@iitkgp.ac.in, nishkalprakash@gmail.com, dsamanta@iitkgp.ac.in, monalisa@iitkgp.ac.in
Cc: ninghui@purdue.edu, fagulpandey@gmail.com, priya.fav67@iitkgp.ac.in, nishkalprakash@gmail.com, dsamanta@iitkgp.ac.in, monalisa@iitkgp.ac.in

03-Nov-2022

Dear Authors:

this email concerns your submission # TOPS-2022-07-0137 titled:

"Private Key Generation from Fingerprint Using Hybrid Feature Vector for Privacy and Security Applications"

I regret to inform you that, in light of the reviews (enclosed below) and the Associate Editor's recommendation, your submission can not be accepted for publication.

I noted that the third review contains very little content, but a Reject Decision would have been reached based on the other two reviews. Essentially the third reviewer believes that using Fingerprint to generate binary sequences is not a new idea.

Thank you for considering ACM Transactions on Privacy and Security.

Sincerely,
Prof. Ninghui Li
Editor in Chief, ACM Transactions on Privacy and Security

=========
AE Comments:
=========

Associate Editor
Comments to the Author:
All reviewers raise significant concerns with the manuscript. The authors are recommended to take the feedback into account as they revise the work for a future submission. Thanks!

==============
Reviewers' Comments:
==============

Reviewer: 1

Recommendation: Reject

Comments:
Yes

Confidential Comments to the Editor
Willing to review a revision. It is not clear to me that the authors can formalize security and what is being claimed. They've been given this feedback before which makes me doubtful.

Comments to the Author
This paper proposes a feature extractor for the fingerprint. This feature extractor has several components:

* A region identification
* A Delauney triangulation network
* A texture feature extractor
* A genetic algorithm that chooses the best features from the above

* A binarization step

The result from this feature extractor is then treated as a key for a biometric cryptosystem.

Major concerns:
I have four main concerns when reviewing this paper all of which are serious:
* Security
**The output of a feature extractor cannot be used directly as a cryptographic key. There is no justification for the claim " binary feature vector does not reveal anything about raw biometric feature information" there are multiple works on reversing biometric features back to the original value [1,2, 3]. One needs a cryptographic argument why this cannot be done.
** Similar to the comment above, there's no reason to think that changing the segment length is sufficient to provide new cryptographic key. Understanding Hamming weight between these values is not sufficient. We need to understand the cryptographic strength of these values.
** Prior analysis of fingerprint entropy places estimates at less than 100 bits [4]. You need strong justification that you can extract more than 1000 entropic bits.
** Security analysis in Section 5 is insufficiently formal. Claims should be made about how an attacker with certain capabilities cannot break the system. For example, why should the guessing time be {d1 \choose d2}*2^{d1} rather than the entropy of the fingerprint?
* Statistical Analysis. The statistical analysis are not detailed enough to assess the claims. The only information in 4.4.1 is that "More than 10^6 bits were generated using the proposed key generation approach." Was this generated with random data? Across different individuals of a dataset? Using multiple readings of an fingerprint? There is no way to validate these claims. This holds for all results in Section 4.
* Literature review. While Section 2 reviews prior work on biometric cryptosystems it does not make it clear how the proposed methods differ. Throughout the work there is no discussion about what it new that allows the authors to improve on prior methods. Simply a discussion of what they did.
* Description of methods. There is very little discussion for what is being done in the pictured algorithms. This connects to the prior point that the authors don't clear distinguish between prior work and their contribution. Its difficult to understand what about their methods yields the dramatic improvement over prior work.

My main recommendation to the authors is to present the work solely as a feature extractor for fingerprints. If you want to claim this is a biometric cryptosystem your security arguments need to be much more formal.

Citations

[1] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. From the iriscode to the iris: A new vulnerability of iris recognition systems. Black Hat Briefings USA,
1, 2012.
[2] S. Ahmad and B. Fuller, "Resist: Reconstruction of irises from templates," in International Joint Conference on Biometrics, 2020
[3] S. Ahmad, K. Mahmood, and B. Fuller "Inverting Biometric Models with Fewer Samples: Incorporating the Output of Multiple Models" in International Joint Conference on Biometrics, 2022.
[4] Matthew R Young, Stephen J Elliott, Catherine J Tilton, and James E Goldman. Entropy of fingerprints. International Journal of Science, Engineering and Computer Technology, 3(2):43, 2013.

Additional Questions:
Does the paper present innovative ideas or material?: Yes

In what ways does this paper advance the field?: Difficult to tell in current state as there is no clear indication what is new compared to prior art.

Is the information in the paper sound, factual, and accurate?: No

If not, please explain why.: Security claims are not justified and untrue in some cases.

Does this paper cite and use appropriate references?: Yes

If not, what important references are missing?: See comments below

Is the treatment of the subject complete?: No

If not, What important details / ideas/ analyses are missing?: See comments below.

Should anything be deleted from or condensed in the paper?: No

If so, please explain.:

Please help ACM create a more efficient time-to-publication process: Using your best judgment, what amount of copy editing do you think this paper needs?: Moderate

Most ACM journal papers are researcher-oriented. Is this paper of potential interest to developers and engineers?: Yes

Reviewer: 2

Recommendation: Major Revision

Comments:
This paper proposes using a novel feature selection mechanism for generating cryptographic keys from fingerprint biometrics. Although the construction and the analyses are done in pretty extensive way, there are some important issues to be considered further.

There is a huge literature about deriving crypto keys from biometric traits, especially from fingerprints. Although a literature survey is given in the paper, it is not so comprehensive and more importantly it does not put forward necessity for such a new work in the area. I'd recommend the authors enhance the literature review by keeping the connection with the proposed work and how it fills a gap.

Algorithmic details of GLCM is missing. Moreover, the motivation behind using correlation, homogeneity and energy features and the rationale behind the formulations are not given.

Most of the sub-mechanisms of consistent region selection (3.2) are taken from literature but it was not clear to me which exact parts are original, which parts are taken. This is a must to assess originality.

It is not a good idea to assume that the readers can read and understand formally explained algorithms. For example, verbal explanation for Algorithm 1 is missing and it does not help the readers. Moreover, steps 8-11 of Algorithm 1 is not comprehensible.

Not only in Algorithm 1, almost in all algorithms, the authors opted not to use textual explanations or use unintuitive explanations. This really worsens the readability of the paper. More importantly, relationships among the algorithms are not clear. Thus it is not so possible to get the big picture.

Another important issue is that it is not clear to me how large amount of bits are obtained per fingerprint. Since for statistical randomness tests up to 10^6 bits are needed, this becomes an important question to answer. Actually not only for randomness tests, but also for cryptographic strength the key size is important.

Although the average values reported for dissimilarity is acceptable, Fig. 10 shows irregularity which is not that good. A justification or explanation is needed for this.

To me, the most important flaw in the paper is that the fact of not being able to guarantee generating the same key (exactly the same bit string) for the same person with different valid fingerprints. Without a clear solution to that problem, practicality of the proposal is not guaranteed. Note. maybe the kgr metric is that metric; however, with the given limited explanation of what it is, I thought that kgr is the metric of same key derivation rate from the same fingerprint of the person.

In the performance evaluation, the methodology for calculating FAR and FRR must be given in much more detail. Here, I do not mean to give the formulas for them, but processing related issues.

Section 4.5 (Comparison with others) is too shallow.

Security Analyses given Section 5 needs more formal treatment. In its current form (especially Sections 5.1 and 5.5) it lacks formalism.

Minor issues:
Keywords: crypto-bimetric --> crypto-biometric

References needed for the arguments in the first two sentences of Section 3.2.2.

Additional Questions:
Does the paper present innovative ideas or material?: Yes

In what ways does this paper advance the field?: This paper proposes using innovative features for fingerprint biometrics to be converted into crypto keys.

Is the information in the paper sound, factual, and accurate?: Yes

If not, please explain why.:

Does this paper cite and use appropriate references?: No

If not, what important references are missing?: There are several papers about key generation using biometrics (incl. some surveys) missing in the lit. review.

Is the treatment of the subject complete?: No

If not, What important details / ideas/ analyses are missing?: Generally, connections between the algorithms and their textual explanations are missing. It is hard to understand the general idea.

The use of the generated key in practical key establishment protocols has not been given in an acceptable way.

Security and privacy analyses are shallow

Please see the author comments section for details.

Should anything be deleted from or condensed in the paper?: No

If so, please explain.:

Please help ACM create a more efficient time-to-publication process: Using your best judgment, what amount of copy editing do you think this paper needs?: Moderate

Most ACM journal papers are researcher-oriented. Is this paper of potential interest to developers and engineers?: Maybe

Reviewer: 3

Recommendation: Reject

Comments:
(There are no comments.)

Additional Questions:
Does the paper present innovative ideas or material?: No

In what ways does this paper advance the field?:

Is the information in the paper sound, factual, and accurate?: Yes

If not, please explain why.:

Does this paper cite and use appropriate references?: No

If not, what important references are missing?:

Is the treatment of the subject complete?: No

If not, What important details / ideas/ analyses are missing?: Fingerprint is unique, so it only can be used to authenticate in the security.

Should anything be deleted from or condensed in the paper?: No

If so, please explain.:

Please help ACM create a more efficient time-to-publication process: Using your best judgment, what amount of copy editing do you think this paper needs?: Moderate

Most ACM journal papers are researcher-oriented. Is this paper of potential interest to developers and engineers?: No