“A Survey On Biometric Template Protection Using Hybrid Approach”

Nishant Kaushal[1], Dr. Sukhwinder Singh[2]

Abstract: Living in an era of technology, where almost everything has become digital and connected worldwide. Mankind needed to maintain its own personal identity among the masses. This all started in the 20th century when criminal cases were being solved using fingerprint matching technique. But soon biometrics was also used in authentication process of individuals for example in airport security and adhaar Id based systems. And then the need of securing the biometric features of individuals became a major concern, with time various biometric template protection schemes were proposed. This paper presents a review of such template protection schemes which are highly acceptable.

Introduction: Biometrics are nowadays used in many applications but its use in security purposes have become a necessity. An efficient biometric template protection technique must follow the following four criteria:
•Diversity: Different templates can be generated from a particular biometric data.
•Revocability: Compromised template cannot be used to get other templates and can also be replaced with new template derived from same original biometric data.
•Non-reversibility: The technique should not allow to recover original biometric data from the transformed template.
• Accuracy: The technique should increase accuracy by reducing false match rates inaccurate rejection rates.
During recent times tremendous work has been done on cancellable templates, fused structures and chaff point generation mechanism for improving fuzzy vault security.
In this paper a detailed survey on these techniques has been done:-

1. Securing fingerprint templates using fused structures.
2. Constructing cancellable template with synthetic minutiae.

Basic Background

For biometrics we have basically two following classifications[1]:

- **Physical biometrics**. Biometric features inherent to the physiological characteristics of an individual that could be considered unique, e.g, face, fingerprint, hand biometrics (hand geometry, palmprint, hand vein) and ocular biometrics (iris, retina).
- **Behavioural biometrics**. Biometric features related to an individual’s action/gestures can differentiate an individual, e.g. written signatures, keystroke patterns, gait and voice.

Figure 1 shows basic biometric system. The process starts with **enrollment**, in which the biometric data is collected using a sensor, extracts features and store it in a biometric template. Usually enrollment takes place once, but in special cases, it can be specifically updated, if that biometric trait changed significantly. In subsequent day to day usage, a user presents his biometric to the sensor and feature extraction is performed.

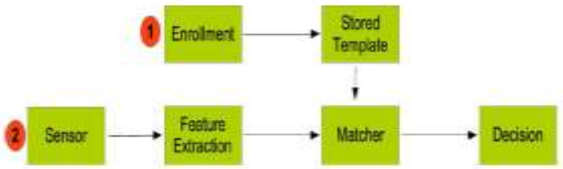


Fig. 1 Biometric enrollment and authentication process[2]

The matcher module will compare the sample with the stored template and make a decision of accept or reject. The biometric features variations of the same biometric trait from the same user is called **intra-class variation**, as opposed to **inter-class variation** which relates to different users. A useful biometric template has small intraclass variation and large inter-class variations[3]. When two biometric samples for the same trait are matched they are given a match score, which must exceed a certain threshold to be considered authentic. Depending on the origin of the samples this score can be: genuine score if the biometric samples are from the same user or impostor score otherwise. A biometric system can function in verification or identification mode. Verification mode confirms the user's identity, by comparing the input with a stored template of that user. Identification mode tries to find out who user is by comparing the input sample against the entire template database.
Given the variability involved with the capture of any biometric the matching function always allows for some threshold of difference between the input and the stored template. Given that it is not feasible to consistently achieve a 100% match and that there is an error threshold the system could make an incorrect decision. As such, regardless of the type of biometric system used, single or multiple, the systems performance is usually evaluated in terms of accepted quality metrics. These metrics are well known so we mention them only briefly: False Match Rate (FMR)[3], False Acceptance Rate (FAR), False Reject Rate (FRR), Genuine Acceptance Rate (GAR), Equal Error Rate (EER), Failure To Enroll (FTE), Failure to Capture (FTC), system matching and enrollment speed and upper bound. The last metric calculates the maximum number of patterns the biometric system is able to recognize. The difference between FMR and FAR is FMR doesn't include previously rejected samples due to image quality or FTC, and this is the reason some authors agree that FMR is a better metric.

Template security

For some time experts believed that the original biometric data can't be reconstructed from a stored template, but[4] [5], to name a few, proved otherwise. To protect against template compromise, encryption was proposed, but it was proven that biometric recognition can't be performed in the encrypted domain[5]. Storage on tamper resistant devices, like smart cards[6], might be feasible for a single template for verification but cannot secure larger template databases. Even though cancelable biometrics[2] or private templates[7], were proposed a long time ago, most of the biometric systems still store insecure templates in the database. When this happens, the security of the multibiometric system resumes to database security, and the argument that multi-modal biometric systems are more secure, doesn't stand. Actually, in the case of multi-modal biometrics, a database breach is even more dangerous, because multiple biometric traits are compromised.

Ratha et al. [2] introduced the concept of cancelable biometrics as shown in table 1 which can be a solution to the problems presented above. Later, template protection schemes were divided into two main groups: cancelable transformations and biometric cryptosystems, depicted in Figure 2.

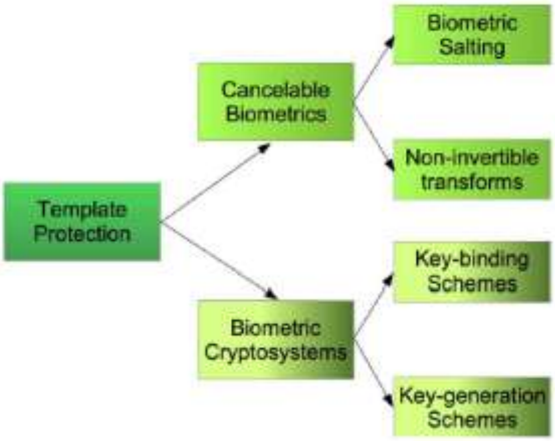
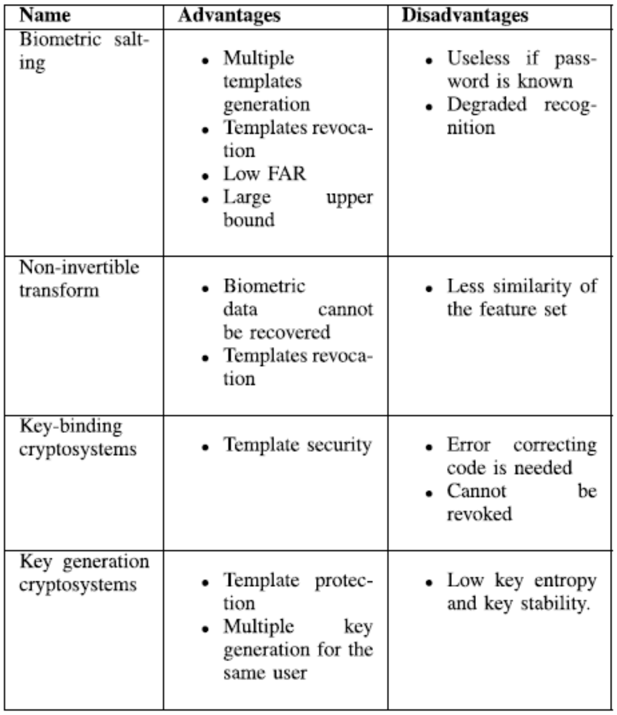


Fig. 2 Biometric template protection[2]



Name	Advantages	Disadvantages
Biometric salting	• Multiple templates generation • Templates revocation • Low FAR • Large upper bound	• Useless if password is known • Degraded recognition
Non-invertible transform	• Biometric data cannot be recovered • Templates revocation	• Less similarity of the feature set
Key-binding cryptosystems	• Template security	• Error correcting code is needed • Cannot be revoked
Key generation cryptosystems	• Template protection • Multiple key generation for the same user	• Low key entropy and key stability.

Table 1. Summary of template protection

Securing fingerprint templates using fused structures :-

In this research article Sandhya and Prasad proposed a technique to secure fingerprint template using fused structures. The transformed features of fingerprint image namely: local structure (LS) and distant structure (DS). Thee structures include all minutiae points of a fingerprint image. These two structures are fused at feature level by generating bit strings and the performance evaluation is done on the basis of equal error rate (EER), separability (d') and Kolmogorov-Smirnov (KS) test results.

Fig. 3 represents the overall framework for the proposed method that contains the following steps:

1. Computation of transformed features (LS and DS) for minutiae points.
2. Representing LS and DS as bit strings.
3. Generating fused bit-string (B_{fus}).

4. Cancelable template generation.
5. Matching.

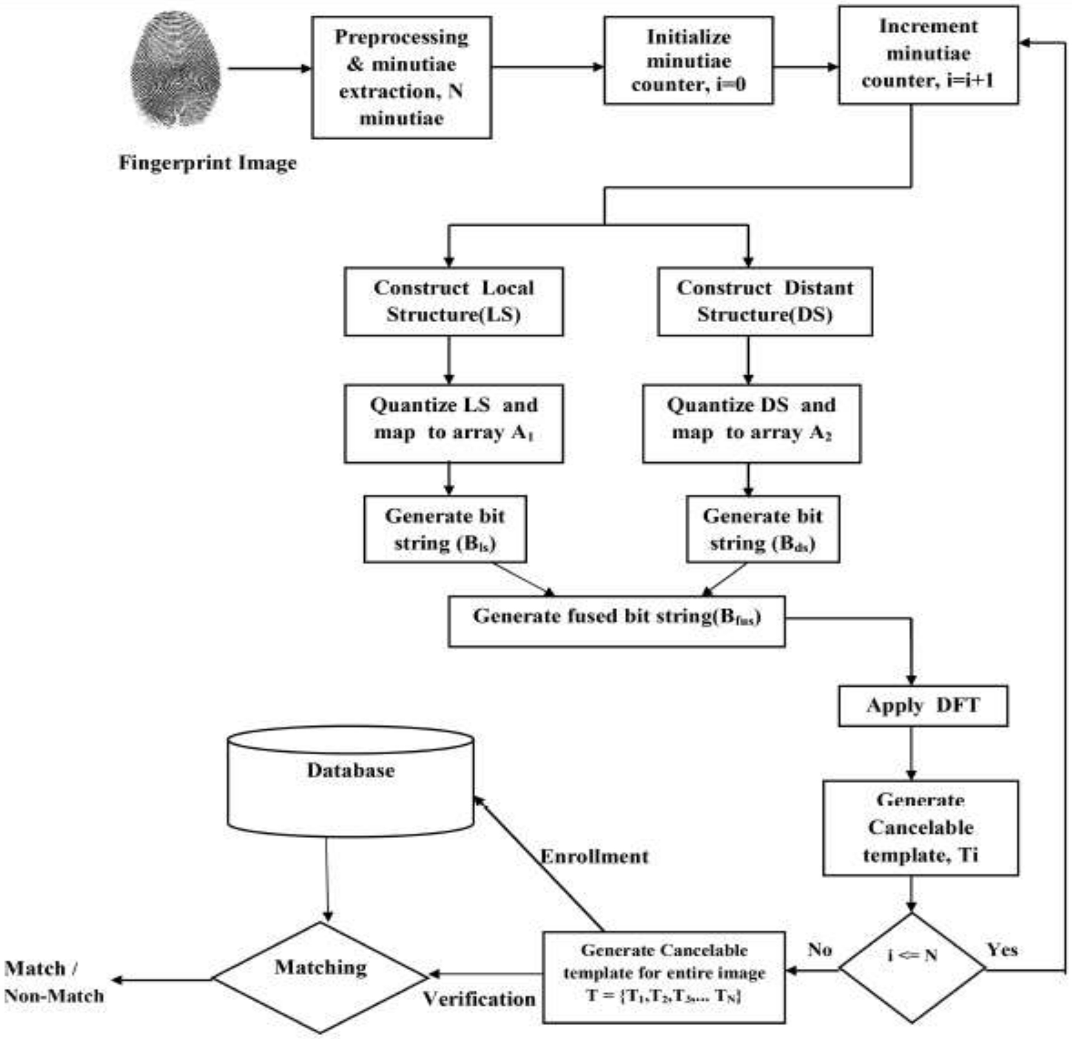

Fingerprint Image
Preprocessing & minutiae extraction, N minutiae
Initialize minutiae counter, i=0
Increment minutiae counter, i=i+1
Construct Local Structure(LS)
Construct Distant Structure(DS)
Quantize LS and map to array A₁
Quantize DS and map to array A₂
Generate bit string (B_ls)
Generate bit string (B_ds)
Generate fused bit string(B_fus)
Apply DFT
Generate Cancelable template, Ti
i <= N
Yes
No
Generate Cancelable template for entire image T = {T₁,T₂,T₃,... T_N}
Enrollment
Database
Verification
Matching
Match / Non-Match

Fig. 3 Overall framework of the proposed method.[8]

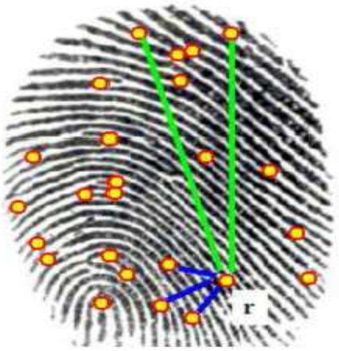


Fig. 4 Representation of LS_r and DS_r for reference minutiae point r with p=3 and q=2, where p represents the number of nearest points considered for construction of LS and q represents the number of farthest points considered for construction of DS.[8]

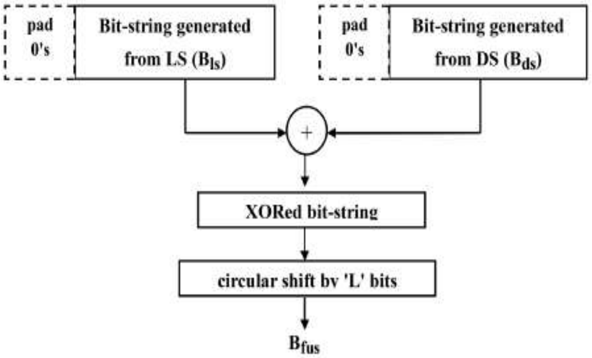

pad
0's
Bit-string generated from LS (B_{ls})
pad
0's
Bit-string generated from DS (B_{ds})
+
XORed bit-string
circular shift by 'L' bits
B_{fus}

Fig. 5 Generating fused bit-string (B_{fus})[8]

Experimental results

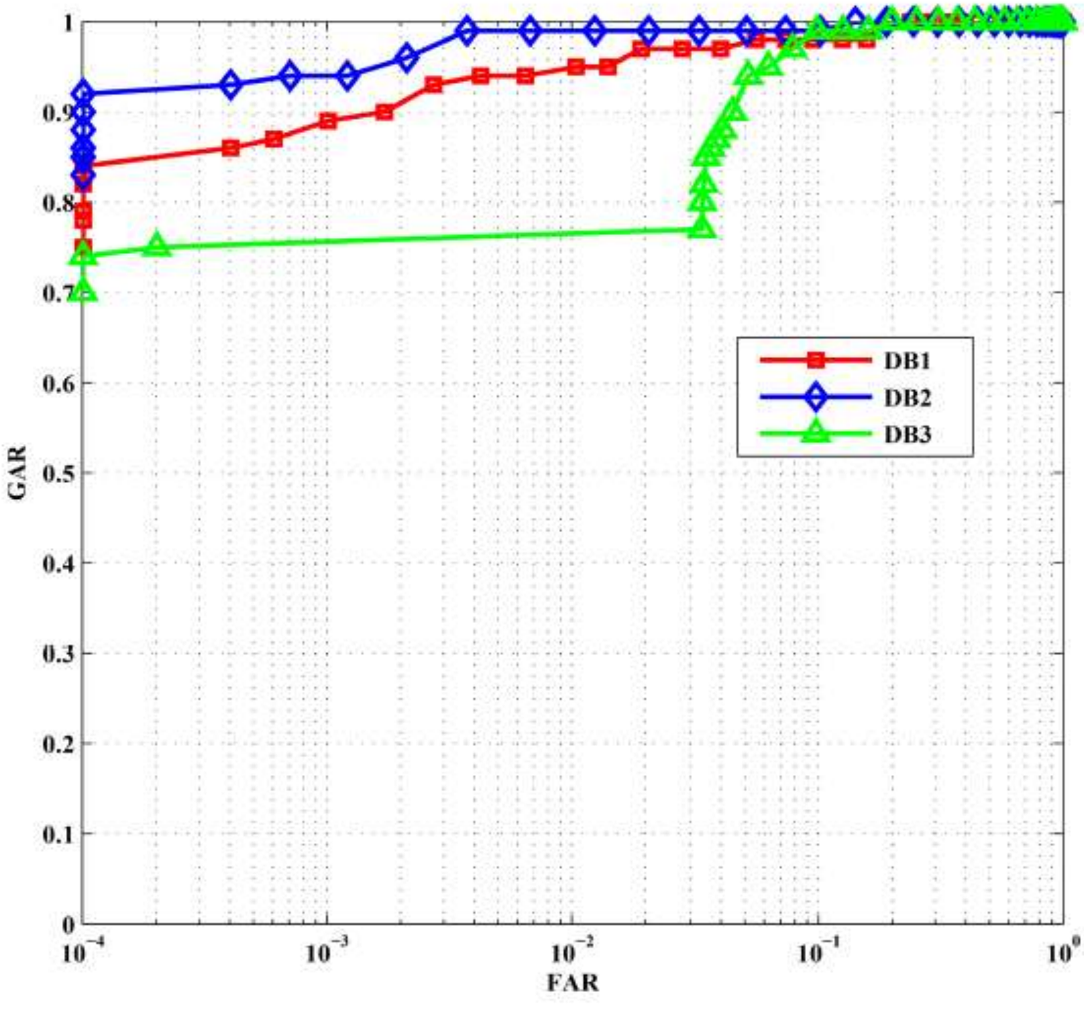


Fig. 6 ROC curves of FVC 2002 databases.[8]

Experimental results prove the tenability of securing fingerprint templates using fused structures.

Cancelable fuzzy vault with periodic transformation for biometric template protection

Dang, Truong, Le and H Truong proposed this method to combine a transformation function and a fuzzy vault system. The transformation function possesses two important properties. The first one is the non-invertible property to protect the biometric template. The second one is to preserve the similarity of distances among transformed templates and among original templates. That means for two same original templates their transformed templates must be similar and vice versa and hence these transformed templates can be used in fuzzy vault. First a feature vector **X** is transformed using a function to obtain **Y.** After that, **Y** is given as input to the fuzzy vault.

During authentication user's feature vector **X'** must be similar to original feature vector **X**. If two same feature vectors are used the fuzzy vault[9] is possible to recover exactly the original key (K'=K) if vector **Y'** is close enough to vector **Y**. Therefore, hash values of K and K' are used during authentication process.

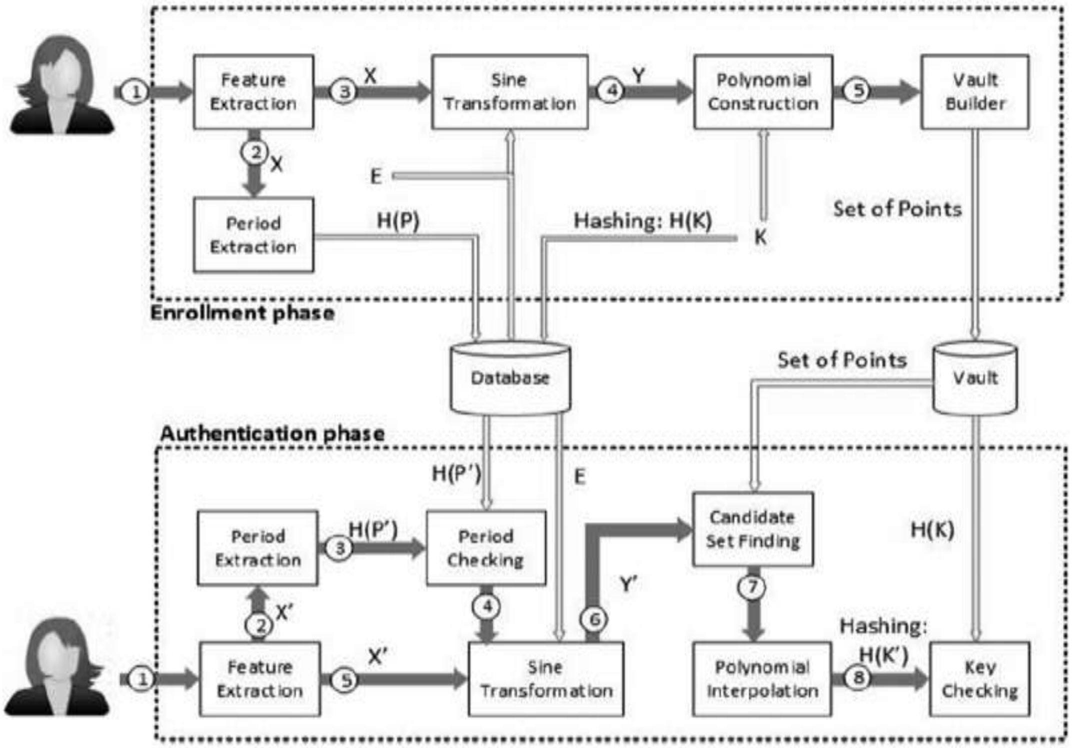


Fig. 7 General architecture.[10]

Evaluation

Tested under Face 94 database[11] the false acceptance rate (FAR) and (FRR) are measured.

- The FAR defines the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the per cent of invalid inputs which are incorrectly accepted.
- By analogy, the FRR defines the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the per cent of valid inputs which are incorrectly rejected.

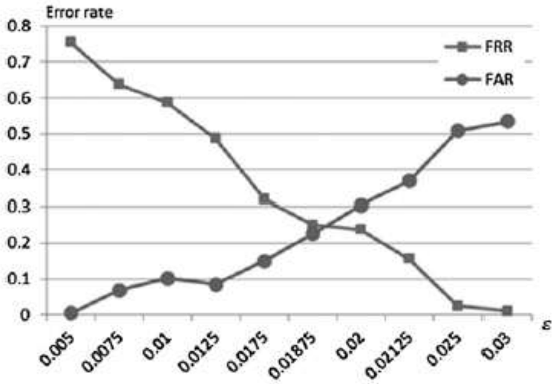


Fig. 8 FAR and FRR (correcting up to three periods).[10]

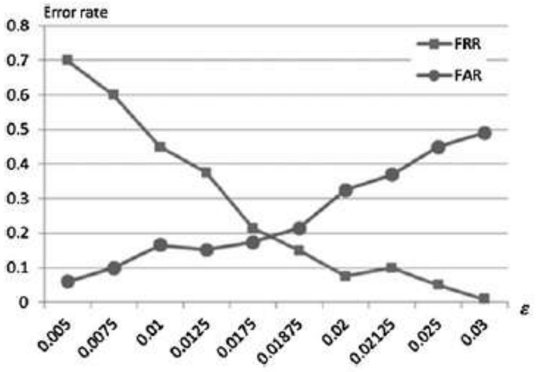


Fig. 9 FAR and FRR with cosine function (correcting up to four periods).[10]

Conclusion

Due to advances in technology and the needs for more secure systems, biometrics systems are becoming widely used. This paper gives an overview on biometric template protection approaches. This is a useful reference for designers implementing new systems, especially in systems with resource constraints, such as embedded and mobile devices.

References

[1] H. Almahafzah and M. Z. Alrwashdeh, ‘A Survey of Multibiometric Systems’, *Int. J. Comput. Appl.*, vol. 43, no. 15, pp. 36–43, Apr. 2012.

[2] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, ‘Generating Cancelable Fingerprint Templates’, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[3] *Handbook of Biometrics | Anil Jain | Springer*. .

[4] A. Ross, J. Shah, and A. K. Jain, ‘From Template to Image: Reconstructing Fingerprints from Minutiae Points’, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[5] A. K. Jain, K. Nandakumar, and A. Nagar, ‘Biometric Template Security’, *EURASIP J Adv Signal Process*, vol. 2008, p. 113:1–113:17, Jan. 2008.

[6] ‘Attacking smart card systems: Theory and practice - ScienceDirect’. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S136341270900017X. [Accessed: 15-Mar-2018].

[7] ‘On Enabling Secure Applications Through Off-Line Biometric Identification - Semantic Scholar’. [Online]. Available: /paper/On-Enabling-Secure-Applications-Through-Off-Line-B-Davida-Frankel/06d81dff121f7bbe3aac5a2c5e89c7d68c739069. [Accessed: 15-Mar-2018].

[8] M. Sandhya and M. V. N. K. Prasad, ‘Securing fingerprint templates using fused structures’, *IET Biom.*, vol. 6, no. 3, pp. 173–182, 2017.

[9] A. Juels and M. Sudan, ‘A fuzzy vault scheme’, in *Proceedings IEEE International Symposium on Information Theory*, 2002, p. 408-.

[10] T. K. Dang, Q. C. Truong, T. T. B. Le, and H. Truong, ‘Cancellable fuzzy vault with periodic transformation for biometric template protection’, *IET Biom.*, vol. 5, no. 3, pp. 229–235, 2016.

[11] ‘Face Recognition Data’. [Online]. Available: http://cswww.essex.ac.uk/mv/allfaces/faces94.html. [Accessed: 15-Mar-2018].