Report

Biometric Template Security using Fuzzy Vault

Avishek Arora [2021JCS2236]

Arihant Jammar [2022JCS2669]

Biometric Security [SIL775]

The Fuzzy Vault is a cryptographic technique used for securing biometric templates. Biometric data such as fingerprint or palmprint are unique to individuals and can be used to authenticate them. However, biometric templates are sensitive information and need to be protected from unauthorized access. The Fuzzy Vault provides a way to protect biometric templates by encoding them with a secret key, which can only be decoded by the authorized user.

The Fuzzy Vault is based on the concept of error-correcting codes, which are used to correct errors that may occur during the transmission or storage of data. In the Fuzzy Vault, the biometric template is encoded with a polynomial equation and a key, which together form the secret Vault. The vault can be only be used by the authorized user to access the key.

To implement the Fuzzy Vault, the following steps are followed:

1: The first step is to extract the biometric features from the raw biometric data. This involves identifying the relevant features, such as the minutiae points, orientation field in the fingerprint, or the palmprint.

2: Once the biometric features have been extracted only few of them are selected as per the Fuzzy Vault parameter r (#f minutiae points considered for generation of vault)

3: These points are normalized as per the parameters B_u, B_v, B_theta.

4: Now we generate a user specific key of length 16*16 bits and generate a CRC checksum for it and in all generate a 272 bit key.

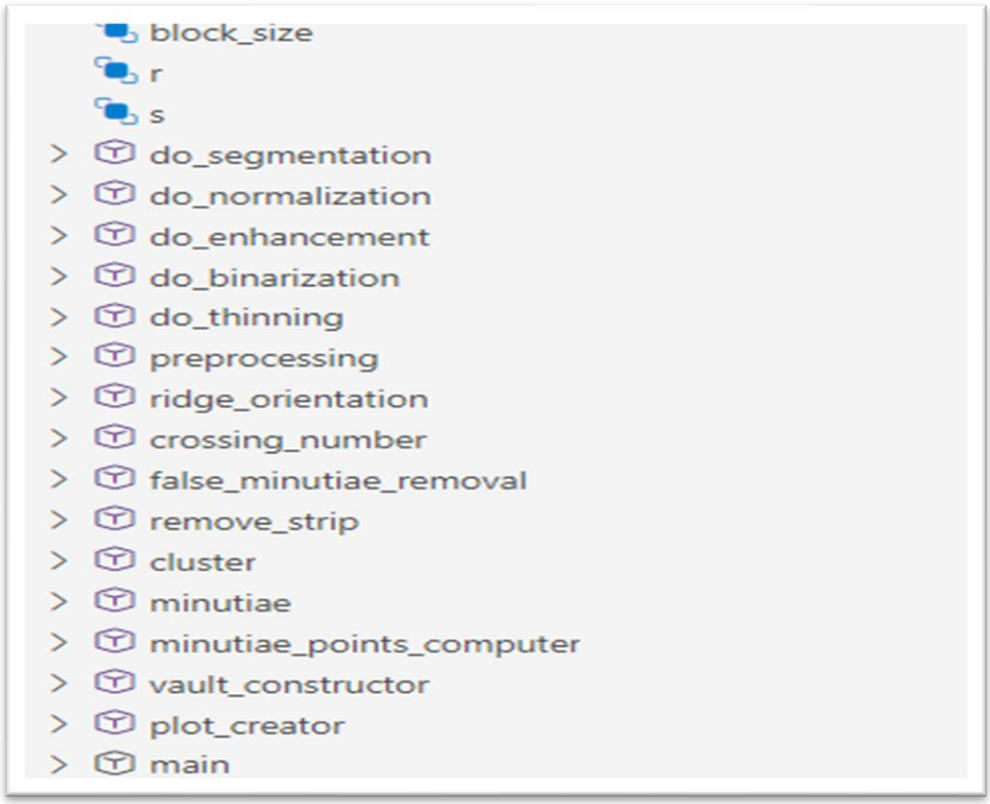
5: This key is used to generate a polynomial of degree 16 whose coefficients are the 272 bits equally divided into 16 bits each and converted into decimal values.

6: Now Galois Field $GF(2^{16})$ is used to encode the feature points and generate the evaluation of these points.

7: To provide security chaff points are added as per security parameter “s” of Fuzzy Vault (#f chaff points added) and the chaff point (a,b) should not be equal to (m,n) where m is a feature point and n is it’s polynomial evaluation and $a \neq m \; and \; b \neq n$.

8: These points are combined together to form the Fuzzy Vault V.

We have provided the implementation of the fuzzy vault encoding, which takes Fingerprint image and Palm Print image of a person and generates a unique keys and generates it’s vault V. (As per research paper)



This image gives an outline of all the functions and global parameters used in the implementation.

```
key = np.random.randint(2, size=16*16,dtype='uint16')
```

The logic used above is used to generate a user specific key.

```
def main():
    img_fp = np.array(cv2.imread("fingerprint.tif",0))
    minutiae_points=minutiae_points_computer(img_fp)
    Vault_fp,vault_fp_print=vault_constructor(minutiae_points,img_fp)

    img_pp = np.array(cv2.imread("palmprint.tif",0))
    minutiae_points=minutiae_points_computer(img_pp)
    Vault_pp,vault_pp_print=vault_constructor(minutiae_points,img_pp)
    x,y=plot_creator(vault_fp_print,vault_pp_print)
    plt.scatter(x,y)
    plt.xlabel('X-axis')
    plt.ylabel('Y-axis')
    plt.title('2D Graph')
    plt.show()
```

In the main function img_fp stores the fingerprint image and img_pp stores the palmprint features as a numpy array. Calls are made to minutie_points_computer to get the minutiae_points.

These minutiae_points act as an input parameter alomg with img_fp/img_pp on a call to vault_constructor function which returns the vault and points for plotting the points.

Matplotlib function plt is used to print the scatter plot.

The python libraries used in the implementation are as follows:

1: numpy

2: cv2

3: math

4: fingerprint_enhancer

5: scikit-learn

6: galois

7: crc

8: matplotlib

9: warnings

The Fuzzy Vault parameters r and s are assigned values 20 and 180 respectively.

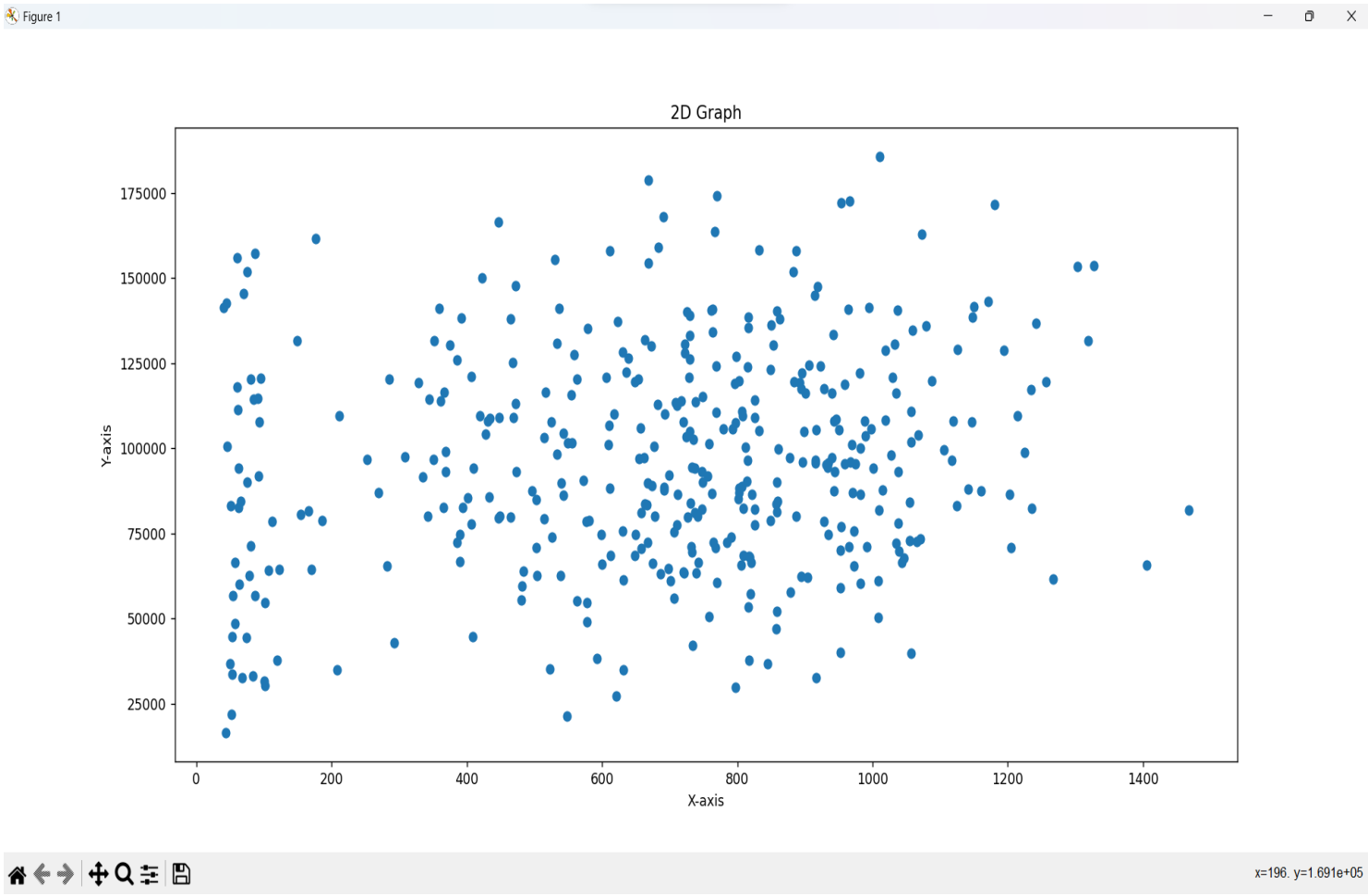
B_u= 6 bits

B_v= 6 bits

B_theta= 4 bits

Sum= B_u + B_v + B_theta =16 bits

block_size=16 considered for minutiae points extraction.



This plot is the output produced when the code has been run. It is a scatter plot containing the genuine and chaff points which overall hides the genuine minutiae points.

This is a multimodal fuzzy vault created with fingerprint and palmprint which increases the security of templates.

Overall, the Fuzzy Vault is an effective technique for securing biometric templates. By encoding the templates with a secret key, the Fuzzy Vault provides a

way to protect sensitive biometric data from unauthorized access.

References:

[1] K. Nandakumar, A. K. Jain and S. Pankanti, “Fingerprint-based Fuzzy Vault: Implementation and Performance”, IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744–757, 2007.

[2] A. Juels and M. Sudan, “A Fuzzy Vault Scheme”, Proceedings of IEEE International Symposium on Information Theory, vol. 6, no. 3, pp. 408, 2002.

[3] K. Nandakumar. “Multibiometric System:Fusion Statergies and Template Security”, PhD thesis, Department of Computer Science and Engineering, Michigan State University, January 2008.

[4] V. Evelyn Brindha,” Biometric Template Security using Fuzzy Vault”, 2011 IEEE 15th International Symposium on Consumer Electronics.