

PRIVACY PRESERVING FINGERPRINT AUTHENTICATION BASED ON CANCELABLE BIOMETRICS

A Synopsis

For the award of

Doctor of Philosophy

In

Computer/ IT Engineering

Submitted By:

Shaikh Ayeshabanu Sibgatulla

[179999913028]

Supervisor:

Dr. Vibha Divyesh Patel

Professor,

Head, Information Technology Department

Vishwakarma Government Engineering College (VGEC),

GTU, India.

submitted to



Gujarat Technological University

Ahmedabad, Gujarat, India.

Dr. Vibha D. Patel

Dr. Mehul S. Raval

Dr. Mukesh A. Zaveri

Contents

1	Abstract	3
2	Brief description of a state-of-the-art research topic	3
3	Definition of the Problem	5
4	Objective and Scope of work	6
5	Original contribution by the thesis	6
6	Methodology of Research, Results / Comparisons	6
6.1	Fingerprint Datasets	6
6.2	Cancelable biometric based fingerprint template protection using discrete cosine transform and index of max hashing	7
6.3	Cancelable biometrics for fingerprint template security based on a speeded up robust feature, fast fourier transform, and index of max hashing	11
6.4	Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing	13
7	Achievements with respect to objectives	16
8	Conclusion and Future work	16
8.1	Conclusion	16
8.2	Future work	16
9	List of all publications arising from the thesis	17
9.1	Paper Published	17
	References	17

1 Abstract

The IT security paradigm evolves from secret-based to biometric identity-based. Biometric identification has become gradually more popular in recent years for handheld devices. Privacy-preserving is a key concern when biometrics are used in authentication systems in the present world. Nowadays, the declaration of biometric traits has been imposed not only by the government but by many private entities as well. There are no proper mechanisms or assurance that biometric traits will be protected by these entities. The encryption of biometric traits to avoid privacy attacks is a giant problem. Hence, state-of-the-art safety and security technological solutions must be devised to prevent the loss and misuse of such biometric traits.

In classical authentication systems, either users need to remember a password (knowledge-based identification system) or have to carry ID proof (token-based identification system). Over the last decades, biometric authentication systems have emerged as an alternative to classical authentication systems where your body is your password (e.g., fingerprint, face, or voice). The prime advantage of biometric traits is that they can never be lost or forgotten. On the other hand, if any of the biometric traits get compromised, then the user will not be able to change them like a password. In the real world, while biometric authentication is becoming increasingly popular, the privacy and security risks related to its usage are raising several concerns.

Biometric authentication systems have become more popular nowadays because of mobile and other handheld devices since they eliminate the need for a password or pin to remember. The usage of the internet and other handheld smart devices promotes the theft of users' biometric traits, which frequently results in a loss of privacy. If an intruder hacks biometric traits, there is no way to change the biometric traits of any person because they are permanently attached to them. The biometric traits are not replaceable like passwords; hence, the key research area is privacy preservation. To stop such biometric traits from being stolen or used improperly, secure technology solutions must be developed. Protecting biometric template data is essential for preventing the loss of user privacy and identification. An effective and efficient approach that focuses on the security and privacy issues of biometric traits is required.

The prime threat associated with biometric authentication is identity theft. Any attack that recovers the biometric template may have a serious impact since users cannot change their biometric traits. Hence, biometric templates must be protected in order to thwart any leakage, as biometric traits are extremely susceptible to change. In privacy-preserving biometric authentication systems, the biometric data is stored in a secure form, which transforms the data into a distorted version and also matches the trait in the transformed domain at the time of recognition.

2 Brief description of a state-of-the-art research topic

S. Wang et al. [12] had proposed a partial hadamard transform approach to the design of cancelable fingerprint templates that contain binary biometric representations. In this system, an ef-

efficient partial hadamard transform-based non-invertible transformation method has been proposed to securely protect binary biometric representation in the design of cancelable biometrics.

The hadamard transform is a symmetric, orthogonal, and non-sinusoidal function (i.e. $H_n^{-1} = H_n^T = H_n$). It transforms from a spatial domain to a frequency domain. The H_n , unitary matrices consist of +1, -1, and the recursive transformations are computed using addition and multiplication only, with no multiplication being involved. The hadamard matrix H_n is of dimension $2^n * 2^n$. Where $*$ is the Kronecker product of two matrices. $H_n = H_1 * H_{n-1}$. For a 2D image, the hadamard transform Y of vector X is: $Y = H_n X H_n^T$.

A binary biometric representation in the data domain can be represented by a binary-valued vector.

$$t_d = [d(0), d(1), \dots, d(m-1)]^T, \text{ where, } d(i) \in 0, 1 \quad (1)$$

The entries of the binary vector t_d are either 0 or 1. First, DFT has been applied to sparsely distributed binary biometric representations, which makes the resultant templates more complex because it renders a dense data representation in the transformed domain. The DFT operation can be performed using the powerful FFT algorithm on t_d to get t_D .

$$t_D = F t_d \quad (2)$$

where, $t_D = [D(0), D(1), \dots, D(m-1)]^T$.

After DFT, a non-invertible partial Hadamard transform has been applied to t_D which makes complex resultant templates t_H from which the original vectors cannot be recovered. The length of the vector t_D is N, and suppose a random row vector of length r is denoted by $K = [k_1, k_2, \dots, k_r]$ where $r < N$ and $N = 2^n$. All entries of K are strictly positive integers with $K_i \neq K_j$. This random vector K has been used to construct the sub-matrix of H_n , denoted by H'_n , such that the i^{th} row of the H'_n is the k_i^{th} row of the H_n . For $i \in [1, \dots, r]$, the size of H'_n is $r \times N$.

$$t_H = H'_n t_D \quad (3)$$

M. V. Prasad et al. [19] had proposed the method that generates the cancelable templates without requiring the pre-alignment of the fingerprint based on fingerprint minutiae representation. First, generate a minimum spanning tree for the fingerprint minutiae in a three-dimensional feature space that connects all the minutiae points, and then the two-dimensional feature space is generated based on the chain code representation from the generated MST. A bit string is then generated by mapping the chain code into the 2D array. Minutiae consist of (x, y, θ) , where (x, y) represents the minutiae coordinates and θ denotes the orientation of the minutiae. The set of minutiae is denoted by M.

$$M = \{M_i(x_i, y_i, \theta_i)\}_{i=1}^m \quad (4)$$

where m is the number of minutiae, (x_i, y_i) is the coordinates, and θ_i is the orientation of the i^{th} minutiae. From these minutiae points a spanning tree, which is a connected acyclic subgraph of

the connected graph. MST of the $G = (V, E)$, such that the total weight or the total length of the edges is minimum. Considering the minutiae set M as vertices V . The prim's algorithm has been explored by finding $(m - 1)$ edges from the $m \in e_{ij}$ edges that form the MST, g' with a minimum total weight of $m(m - 1)/2$.

$$g' = \{e_{i_r j_r} : i_r < j_r; r = 1, 2, \dots, m - 1; i_r, j_r = 1, 2, \dots, m\} \quad (5)$$

Now the chain code CC is constructed from the generated MST by pairing up the length L of the edge e_{ij} and the orientation of the starting vertex of the edge θ . After selecting the initial vertex, the tree is traversed by breadth-first search and produces the sequence of edges e_i , where $i=1,2,\dots,m-1$. For each edge e_i with two measurements, the weight of the edge (L_i) and the orientation (θ_i) of the minutiae v_i . Hence the chain of code C_i is the sequence of $(L_1, \theta_1)(L_2, \theta_2) \dots (L_{m-1}, \theta_{m-1})$.

$$C_i = (L_i, \theta_i); i = 1, 2, \dots, m - 1 \quad (6)$$

After the chain code is generated, it is mapped to the 2D array consisting of the small cells. After pairing the length and orientation of minutiae in MST, it can be determined which cell in the 2D array includes minutiae. A 1D bit string $\{h_k\}$ of length $d = M \times N$ is generated by sequentially visiting the cells by a raster scan of the above 2D array, in which at most or less than $(m - 1)$ 1's and all others are 0's. If a cell in the 2D array has one or more minutiae, then the cell is set to 1; otherwise, they are set to 0. The complex-valued vector H is formed from the $\{h_k\}$ in the frequency domain by taking the discrete fourier transform. To add more security, this complex-valued vector H is multiplied by a random matrix key A in order to get the cancelable template $T = AH$.

B. Choudhury et al. [4] had proposed a novel method of non-invertible transformation function using the concepts of steganography, which generates a cancelable biometric template. The combined approach of discrete cosine transformation and huffman coding has been used to get the non-invertible transformation in steganography. The steganography is the covered communication that hides the secret image through an unsuspecting cover image. In secret communication, the secret image is hidden by embedding the least significant bits (LSB_s) of each pixel in the cover image.

3 Definition of the Problem

- Designing a biometric template protection system that provides security without compromising accuracy is challenging.
- It is a complicated task to find an appropriate transformation function for cancelable biometrics because of the intra-class variability of biometric patterns.
- Assume that CT is a cancelable transform that converts biometric z to a cancelable biometric $CT(z)$. The biometric z' 's transformed version, $CT(z)$ should not be identical to the original biometric.

- The inverse transform CT^{-1} should not exist such that the original biometric z should not be revocable from the modified one $CT(z)$.

4 Objective and Scope of work

- To study and explore various existing privacy-preserving approaches and understand their limitations.
- Design a transformation approach for cancelable biometrics such that the templates are easy to revoke, difficult to invert, and do not degrade performance. (e.g., security without compromising accuracy)
- To achieve good performance in terms of the accuracy of biometric systems.
- To discover highly discriminative features of the biometric traits using a learning-based approach, which helps to achieve better accuracy.
- Evaluating the performance of the proposed approaches by comparing them with existing approaches.

5 Original contribution by the thesis

- The thesis work proposes three different approaches that are implemented and compared with other state-of-the-art methods to evaluate their performance.
- The first proposed cancelable biometrics approach is based on a non-invertible transformation function using the concepts of discrete cosine transformation and uniformly random permutation-based index of max hashing.
- The second proposed cancelable biometrics approach is based on a speeded-up robust feature and a fast fourier transform with an index of max hashing.
- The third proposed cancelable biometrics approach is based on a learning based approach using the concept of an autoencoder.

6 Methodology of Research, Results / Comparisons

6.1 Fingerprint Datasets

Dataset	Users	Samples	Resolution	Sensor
FVC2002 DB1	100	8	500 dpi	Optical Sensor
FVC2002 DB2	100	8	569 dpi	Optical Sensor

Table 1: Dataset Summary

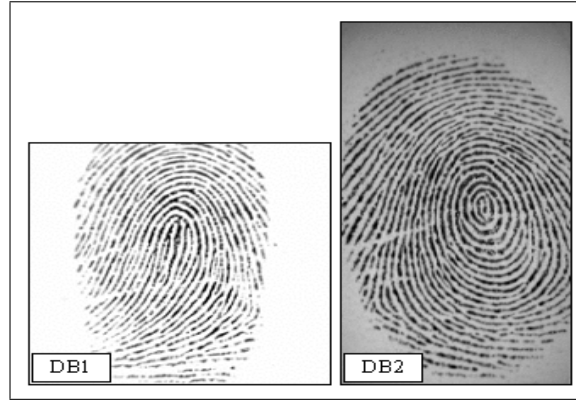


Figure 1: FVC2002 DB1 and FVC2002 DB2 Fingerprint Datasets

6.2 Cancelable biometric based fingerprint template protection using discrete cosine transform and index of max hashing

We have proposed a novel method for cancelable biometrics based on a non-invertible transformation function using the concept of index of max hashing. The combination of a discrete cosine transformation and a uniformly random permutation-based index of max hashing is a non-invertible transformation used in this method. The first discrete cosine transformation has been applied to the fingerprint image, which makes the resultant templates more complex. After discrete cosine transformation, the uniformly random permutation-based index of maxing has been applied in order to get the transformed fingerprint template from which the original fingerprint cannot be recovered.

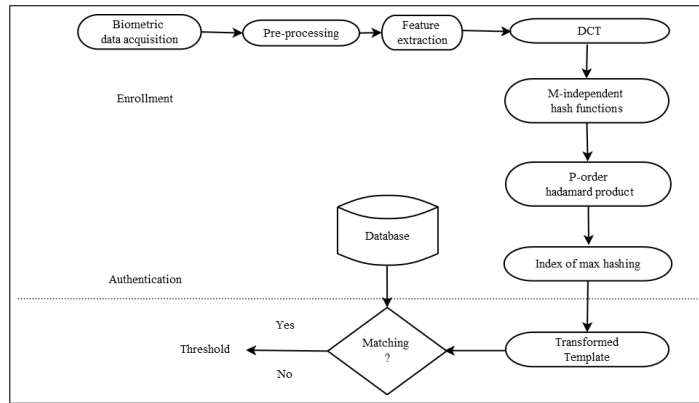


Figure 2: Proposed cancelable biometrics scheme

The proposed algorithm for generating the cancelable fingerprint template can be summarized as the following steps:

- Read the fingerprint image of size $M \times N$. Apply DCT to the fingerprint image, find the minimum value of the DCT coefficients, and subtract the minimum value from all the DCT coefficients to convert the negative values into positive values. The two-dimensional DCT

transforms an image $f(i, j)$ into the frequency domain $F(u, v)$ by an equation given as,

$$F(u, v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i, j) \cos \left[\frac{\pi u(2i+1)}{2M} \right] \cos \left[\frac{\pi v(2j+1)}{2N} \right] \quad (7)$$

where $1 \leq u \leq M-1, 1 \leq v \leq N-1$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, u = 0 \\ \sqrt{\frac{2}{M}}, 1 \leq u \leq M-1 \end{cases}, \alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, v = 0 \\ \sqrt{\frac{2}{N}}, 1 \leq v \leq N-1 \end{cases}$$

- For each hash function $h(x)$, permute the enrolled/query feature vector x randomly for m times, $\hat{x} = \text{perm}(x)$ in order to get the permutation set θ .

$$\{\theta_{(l,i)} | l = 1, \dots, q, i = 1, \dots, m\} \quad (8)$$

- Generate a p-order hadamard product vector by performing element-wise multiplication on the permuted vectors. For $j = 1, \dots, k$, where k is the window size,

$$\bar{x}(j) = \Pi_{l=1}^p (\hat{x}_l(j)) \quad (9)$$

- For each $\bar{x}$, select the first k -elements where $1 < k < d$. Find the maximum entry value within window size k and record its index $t \in [1, k]$ as the hashed code. Repeat the previous steps with different permutation sets $\{\theta_{(l,i)} | l = 1, \dots, q, i = 1, \dots, m\}$ and construct hashed code in order to generate the transformed template.

$$\bar{t} = \{t_i \in [1, k] | i = 1, \dots, m\} \quad (10)$$

The two fingerprint vectors with high similarity give a high probability of collision in the rank domain when index of max hashing is used with ranking-based locality-sensitive hashing. On the other hand, the vectors far apart from each other result in a lower probability of hash collision.

We have tested the effects of different parameters of the index of max hashing with discrete cosine transforms like window size k , hadamard product order p , and the number of hashing functions m . We have checked the performance in terms of EER with respect to the different window sizes k , which varied from 50, 80, 100, 128, 156, 200, and 250, by fixing m at 600 for the hadamard product order $p = [2, 3, 4, 5]$. Both figures show that the EER drops gradually when larger k and p are applied. The small k implies fewer comparisons and is thus less informative of max-ranked features.

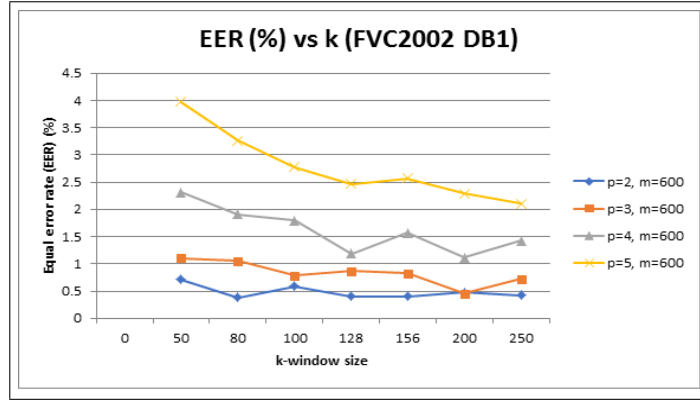


Figure 3: EER (%) vs k on FVC2002(DB1)

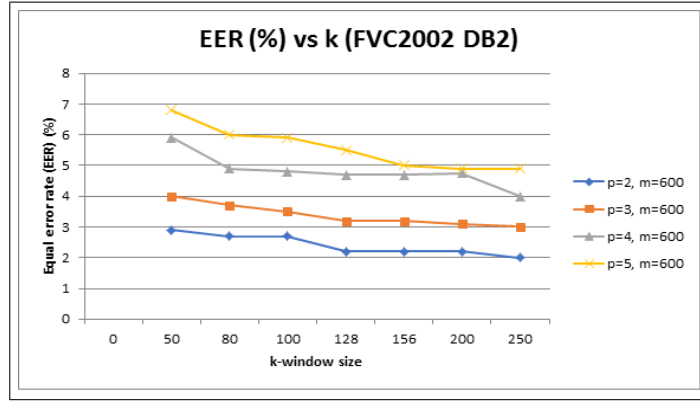


Figure 4: EER (%) vs k on FVC2002(DB2)

The suggested discrete cosine transform approach based on EER performance was further examined in terms of how various independent hashing methods affected the results. Fixing $k = 128$ and $p = 2$, m ranged from 5, 10, 50, 100, 300, 500, 800, and 1000. It is evident from both statistics that an improved EER is achievable in relation to the increment of m . In the worst case, assume that the adversary learns the minimum and maximum values of the feature components of x . Let's take an example of FVC2002 DB1, the minimum and maximum values of the feature components are -0.2504 and 0.2132, respectively. There are a total of 4636 possibilities. In our implementation, the possibility of guessing a single feature component of x requires 4636 attempts (approximately 2^{12}). Thus, the entire 299 feature components require around $2^{12 \times 299} = 2^{3588}$ attempts in total. Obviously, this is computationally infeasible.

To investigate the time efficiency of the proposed method, we record both average code generation and matching time on a machine with specifications such as an Intel CPU i7-7700HQ (2.8 GHz) and 16 GB of RAM. MATLAB Ver. 2016a has been used without optimizing code. The computation time of the hash code generation is longer than that of the matching due to the large number of independent hash functions to be generated, while matching takes much less time with the simple matcher.

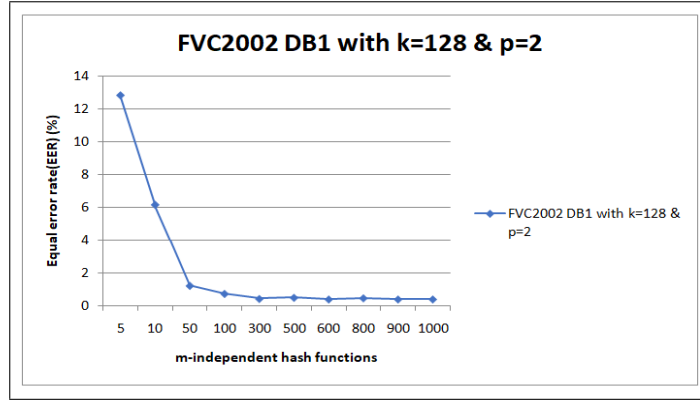


Figure 5: EER (%) vs m-independent hash functions on FVC2002(DB1)

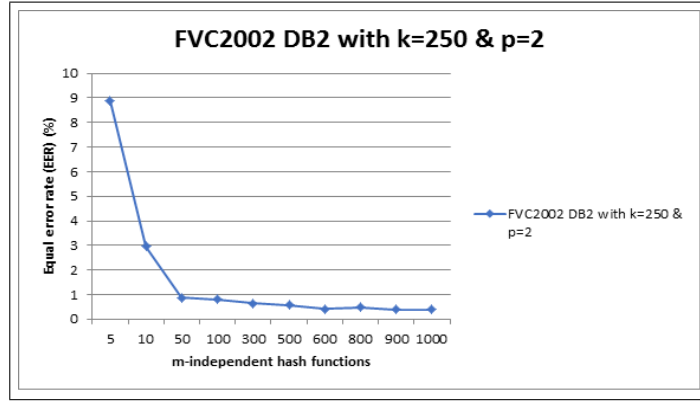


Figure 6: EER (%) vs m-independent hash functions on FVC2002(DB2)

It shows the comparison of different methods of cancelable biometrics and the proposed method. From the table, we can see that the proposed method is performing better than some of the existing methods. Therefore, it can be one of the potential methods for generating transformed templates. Table 2 reports the EER comparison of different state-of-the-art methods that have been tested on DB1. The proposed method used DCT with a uniformly random permutation-based index of max hashing, which gives good EER as compared to different cancelable biometrics methods.

Cancelable biometrics methods	Equal error rate(%)
B. Choudhury et al. [4]	1.2
S. Wang et al. [12]	1.15
M. V. Prasad et al. [19]	1.8
Z. Jin et al. [11]	0.43
Proposed method	0.39

Table 2: Equal error rate(EER) of different cancelable biometric methods

6.3 Cancelable biometrics for fingerprint template security based on a speeded up robust feature, fast fourier transform, and index of max hashing

We proposed a highly secure method for cancelable biometrics using a speeded up robust feature approach for image feature extraction, which is followed by a fast fourier transform with an index of max hashing and a hadamard product for the protection of the biometric template. After extracting features with the speeded up robust features, take the discrete Fourier transform of B_v . The fast fourier transform is used to spread out the spectrum's frequency samples so that they are not sparsely distributed. Select and permute the strongest extracted features. Generate a permutation set θ for each hash function s based on g random permutation.

Using s distinct hash functions $\{hash_i(X), i = 1, \dots, s\}$, randomly permute feature vector B for g times, yielding p permuted vectors, $p = \text{perm}(B)$. To create the h -order hadamard product vector z , element-wise multiply the p permuted vectors. Set $z(j) = \prod_{l=1}^h(p(j))$. The transformation is non-invertible since it is a row-reduced submatrix of H_n and is always column rank deficient, in accordance with the characteristics of the hadamard matrix. Select the first y elements of each z permuted vector, and then record the index of the highest value in c as the hashed code.

Biometric Template Security Algorithm

Input: Input: Fingerprint image of size $M \times N$, FVC2002

Output: Output: Hash Code $c = \{c_i \in [1, y] | i = 1, \dots, s\}$

Step 1: Read the fingerprint image. Extract fingerprint features using speeded-up robust features B_v .

Step 2: Apply the fast fourier transform to the v -dimensional fingerprint feature vector.

Step 3: Select and permute the strongest extracted features. Generate a permutation set θ for each hash function s based on g random permutation.

Step 4: Using s distinct hash functions $\{hash_i(X), i = 1, \dots, s\}$, randomly permute feature vector B for g times, yielding p permuted vectors, $p = \text{perm}(B)$

Step 5: To create the h -order Hadamard product vector z , element-wise multiply the p permuted vectors.

Set $z(j) = \prod_{l=1}^h(p(j))$

Step 6: Select the first y elements of the each z permuted vector.

Step 7: Initialize the i^{th} hash code $c_i = 0$.

Step 8: Within the y items, pick the largest elements.

Step 9: Note the bits for the corresponding index values, c_i .

For $j = 1 \rightarrow y$

If $z(j) \geq z(c_i)$

then $c_i = j$;

Step 10: Repeat m times steps 4 to 8 in order to get a hash code of length s .,

$c = \{c_i \in [1, y] | i = 1, \dots, s\}$

The proposed method of cancelable biometrics has been tested on the FVC2002-DB1 and DB2 datasets. To determine the average EER value, first obtain the EER values for the various authentication thresholds. The EERs for the various thresholds attained using the suggested strategy on the FVC2002-DB1 and DB2 datasets are shown in Figure 7. For the FVC2002-DB1 and DB2 datasets, the average EER is 0.40 and 1.31, respectively. It has been clearly seen that in general, the proposed method on the FVC2002-DB1 dataset has achieved smaller EERs (i.e., higher verification accuracy) than the FVC2002-DB2 dataset. Figure 8 displays the suggested technique's accuracy for various threshold settings. The value of total success rate or accuracy decreases from higher to lower values as the threshold increases.

Non-invertibility enhances the security of the template space by employing a transformation process to reset the order or position of the feature set. It is computationally hard to reconstruct original features with the resulting hash values due to the one-way transformation characteristic of the hashing function. In cases where hash values are compromised, users will be re-enrolled with a new hash function; hence, both non-invertibility and reusability requirements are satisfied. Diversity can also be attained since different hash functions are used for old compromised hash values and new hash values. If both the index of max hash codes and the permutation set θ are revealed, the attack complexity could be significantly reduced. The p-order hadamard product can largely increase the difficulty of such recovery.

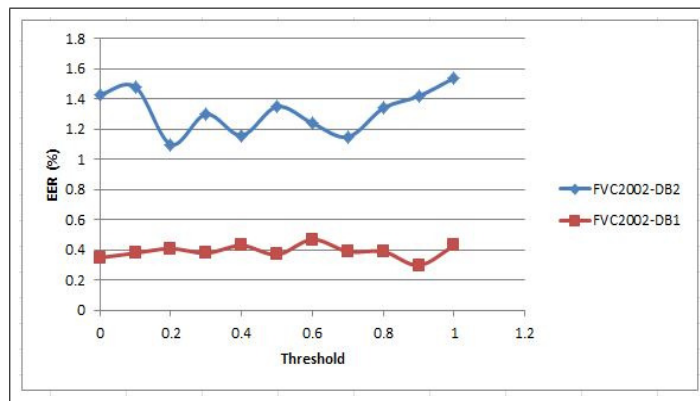


Figure 7: Comparison of EER for the proposed methods on FVC2002 database

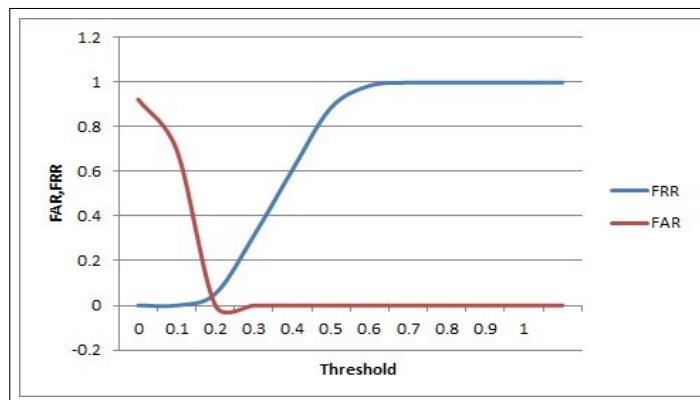


Figure 8: FAR and FRR versus threshold - FVC2002 database

In the proposed method, the index of max hashing provides strong concealment for the biometric traits. This empowers the notion of a non-invertibility guarantee. The index of max hashing is a type of ranking-based hashing method that relies on the relative ordering of feature dimensions, which is independent of the magnitude of the features. It transforms a real-valued feature vector into an index code such that the pairwise-order measure in the hashed codes is closely correlated with the rank similarity measure.

6.4 Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

We propose a convolutional autoencoder and a winner-take-all hashing-based cancelable biometric template. For each image, the latent-space vector representation is computed, and features are extracted using the convolutional autoencoder. The generated biometric feature vector is further enhanced with random noise to increase the discriminative power and enable the revocability of biometric templates. When computing similarity, winner-take-all hashing is used to determine the relevant features and effectively ignore the rest of the information. The cancelable fingerprint template algorithm using convolutional autoencoder, random noise, and winner-take-all hashing has been proposed. The convolutional autoencoder has been used to extract features from the images and represent them in a latent space, which represents the relevant and most useful features. Random noise and winter takes all hashing are used to generate a cancelable template.

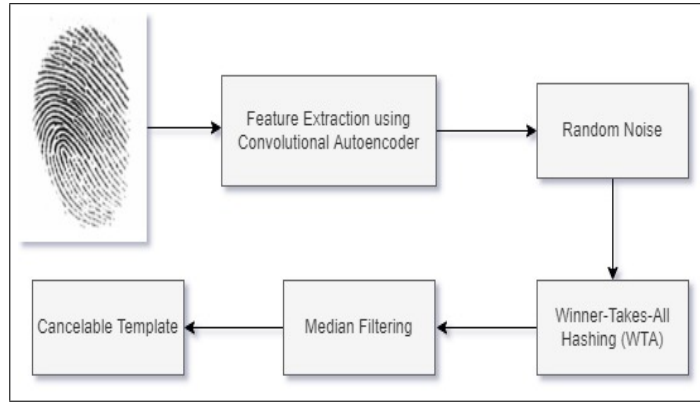


Figure 9: Block diagram of the proposed method

An autoencoder is a type of neural network that can be used to learn a compressed representation of raw data. A convolutional autoencoder is an unsupervised learning technique for neural networks that has been trained to replicate the input image in the output layer. The convolutional autoencoder is used for extracting features from images and compressing them to a lower dimension called latent space. A latent space vector is generated from the input images by extracting the relevant and most useful features required for approximating the images. Winner-take-all hashing is an advanced method used due to its effectiveness in enabling fast similarity searches. The method can be used to generate different sequences based on the number of permutations. It records the position of the highest value of biometric features. This happens after the application

of random permutations.

As shown in Table 3, a winner-take-all hashing example with three input vectors x_1 , x_2 , x_3 , window size K , and one permutation θ . x_1 and x_2 are unrelated and result in different output codes; each element in x_3 has been perturbed by 1, which changes the ranking of the items but keeps the maximum of the first K elements the same, yielding the same code once more.

Table 3: Winner-take-all Hashing

Feature	Permuted Feature based on random permutation set $\theta =$ $\{4, 5, 1, 0, 3, 2\}$	Selected feature based on window size $K=4$	Winner- take-all Hashing $Hwta(Fx)$
$F_{X1} = \{1, 6, 4, 8, 7, 9\}$	$\theta(F_{X1}) = \{7, 9, 6, 1, 8, 4\}$	$F_{S1} = \{7, 9, 6, 1\}$	2
$F_{X2} = \{10, 3, 9, 2, 5, 4\}$	$\theta(F_{X2}) = \{9, 3, 2, 4, 10, 5\}$	$F_{S2} = \{9, 3, 2, 4\}$	1
$F_{X3} = \{2, 7, 4, 9, 8, 10\}$	$\theta(F_{X3}) = \{8, 10, 7, 2, 9, 4\}$	$F_{S3} = \{8, 10, 7, 2\}$	2

This network is implemented using tensorflow and python. The first is an encoder used for compressing the input image by extracting the features using convolution layers. The second is a decoder used for reconstructing the image from the extracted features using transposed convolution layers. Every block of convolution or transposed convolution is followed by LeakyReLU and batch normalization. The network is trained on the FVC2002 dataset. The main purpose of the convolution layer is to extract features from the images of the training set. A filter is used to identify or detect a specific pattern in the input image. The pooling layer decreases the feature map's dimensionality but keeps the key feature in it. The max-pooling layer will downsample the input by two times each time you use it, while the upsampling layer will upsample the input by two times each time it is used.

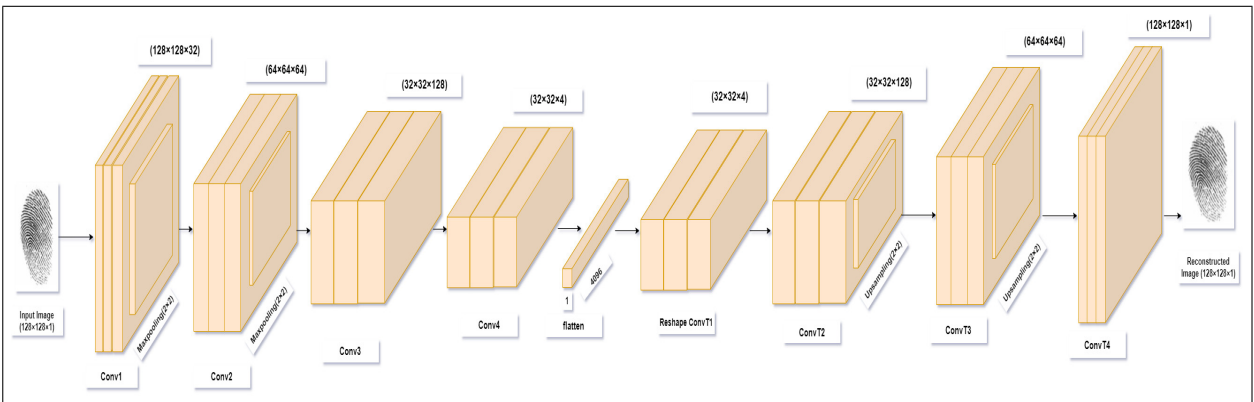


Figure 10: Fingerprint Convolutional Autoencoder Model

The validation loss and the training loss both are in sync. It shows that the model is not overfitting. The validation loss is decreasing and not increasing.

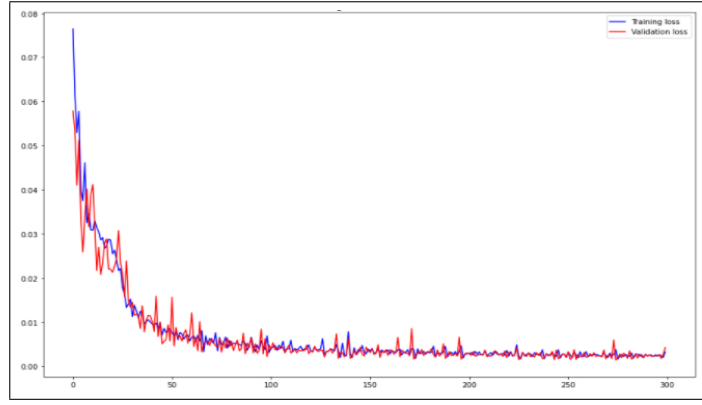


Figure 11: Training and validation loss

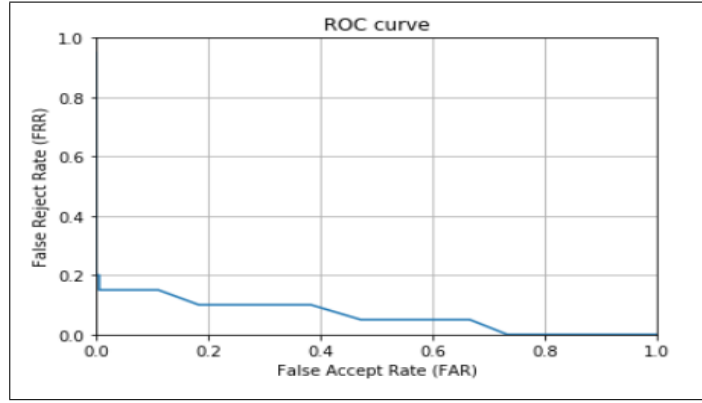


Figure 12: Equal Error Rate (EER%): 0.1306 - FVC2002 DB1

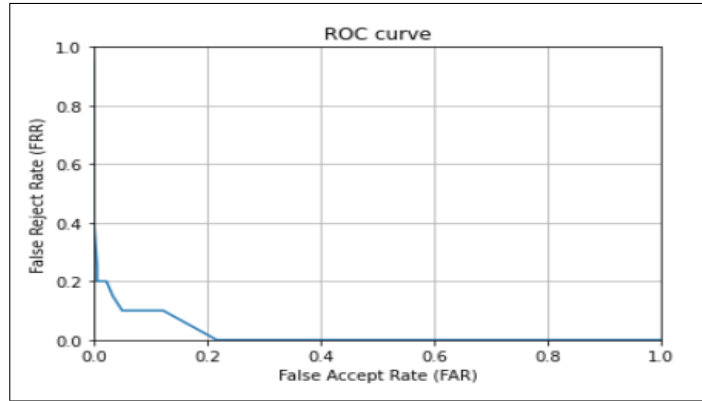


Figure 13: Equal Error Rate (EER%): 0.0861 - FVC2002 DB2

Non-invertibility is an important property to fulfill for every cancelable transformation. Even if it is compromised, invertibility should not be possible (computationally hard). In the proposed method, the final template has been reduced to one-fourth the size of the original biometric image, i.e., from $M \times N$ (here, 224×224) to $M/4 \times N/4$ (here, 56×56). Once a template is generated, regeneration of the original biometric image is not possible without the use of a trained network with known weights. The generated template is median-filtered, which is a non-invertible operation. Therefore, the templates generated in the proposed work are non-invertible.

7 Achievements with respect to objectives

- The research results show that the different transformation approaches for cancelable biometrics can achieve better accuracy and non-invertibility.
- The proposed learning based approach is also implemented and tested with public fingerprint datasets, which achieves better accuracy.
- The proposed privacy-preserving approaches can also improve the accuracy of biometric systems.
- The proposed work can be useful for the biometric template security research community to process the secure privacy-preserving approach.
- As an outcome of the contribution, two journal papers have been published. Another journal paper has been submitted and is under review. The details of publications are given in Section 9.

8 Conclusion and Future work

8.1 Conclusion

Due to the non-revocable nature of the biometric traits, they cannot be replaced if stolen by an adversary. Hence, it would be better to find a solution that gives the security of biometric traits with high accuracy and makes templates as non-invertible and revocable as and when it requires. We presented cancelable template generation using different approaches. The index of maximum hashing, the fast fourier transform, the hadamard product, and speeded-up robust features-based feature extraction are used in this study. According to theoretical reason and actual evidence, the index of maximum hashed codes can substantially maintain performance as a rank correlation attribute. The proposed method is also shown to satisfy non-invertibility template protection criteria. Subject to correctly calibrated parameters, it is also very resistant to several important security and privacy attacks that are now in use. A convolutional autoencoder is used in the suggested method for feature extraction, and winner-take-all hashing with median filtering is used for the creation of cancellable biometric templates. The technique demonstrated effectiveness, non-invertibility, and privacy preservation.

8.2 Future work

The path for our future work will be to continue to push the suggested template protection scheme's limits. In the future, we can put the proposed strategy to the test by combining encryption, watermarking, and steganography techniques for developing efficient cancelable biometric recognition systems. Another challenge is that we may think about extending it to multi-biometrics, where a different biometric modality could be utilized to construct the feature. The other challenge is to cope with record multiplicity attacks such that intruders cannot recover the original biometric template by interlinking the multiple templates from the different applications.

9 List of all publications arising from the thesis

9.1 Paper Published

Published:

- Journal: "Significance of the Transition to Biometric Template Protection: Explore the Future", International Journal of Image and Graphics, Vol. 21, No. 2 (2021) 2150025(17 pages)(ESCI and Scopus Indexed)
- Journal: "Fingerprint Template Protection: Cancelable Biometrics", International Journal of Computational Vision and Robotic (Scopus Indexed (Elsevier))(Accepted)

Submitted:

- Journal: "Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics", Multimedia Tools and Applications (SCI, IF 3.6, EBSCO)

References

- [1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP Journal on advances in signal processing, vol. 2008, (2008)
- [2] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy.," IEEE Computer, vol. 45, (2012)
- [3] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in Security and privacy in Biometrics, Springer, (2013)
- [4] B. Choudhury, P. Then, B. Issac, V. Raman, and M. K. Haldar, "A survey on biometrics and cancelable biometrics systems," International Journal of Image and Graphics, vol. 18, (2018)
- [5] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Transactions on pattern analysis and machine intelligence, vol. 29, (2007)
- [6] E. Pagnin and A. Mitrokovtsa, "Privacy-preserving biometric authentication: challenges and directions," Security and Communication Networks, vol. 2017, (2017)
- [7] M. Joshi, B. Mazumdar, and S. Dey, "Security vulnerabilities against fingerprint biometric system," arXiv preprint arXiv:1805.07116, (2018)
- [8] L. Guo, Y. Mao, and Y. Guo, "Non-invertible fingerprint template protection with polar transformations," in Privacy, Security and Trust (PST), 2016 14th Annual Conference on, IEEE, (2016)
- [9] R. Dwivedi and S. Dey, "A non-invertible cancelable fingerprint template generation based on ridge feature transformation," arXiv preprint arXiv:1805.10853, (2018)

- [10] R. Dwivedi and S. Dey, "Score-level fusion for cancelable multibiometric verification," *Pattern Recognition Letters*, (2018)
- [11] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 13, (2018)
- [12] S. Wang, G. Deng, and J. Hu, "A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognition*, vol. 61, (2017)
- [13] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in *Media Forensics and Security II*, vol. 7541, International Society for Optics and Photonics, (2010)
- [14] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, (2015)
- [15] M. Sandhya and M. V. Prasad, "k-nearest neighborhood structure (k-nns) based alignment-free method for fingerprint template protection," in *Biometrics (ICB), 2015 International Conference on*, IEEE, (2015)
- [16] H. Kaur and P. Khanna, "Gaussian random projection based non-invertible cancelable biometric templates," *Procedia Computer Science*, vol. 54, (2015)
- [17] T. Murakami, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi, "Cancelable indexing based on low-rank approximation of correlation-invariant random filtering for fast and secure biometric identification," *Pattern Recognition Letters*, (2018)
- [18] K. Takahashi and S. Hirata, "Cancelable biometrics with provable security and its application to fingerprint verification," *IEICE Transactions*, vol. 94-A, 233–244, (2011)
- [19] M. V. Prasad, P. Swathi, C. R. Rao, and B. Deekshatulu, "Minimum spanning tree (mst) based techniques for generation of cancelable fingerprint templates," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 28, (2014)
- [20] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, 2004.
- [21] A. Ross, K. Nandakumar, and A. K. Jain, "Introduction to multibiometrics," in *Handbook of biometrics*, pp. 271–292, Springer, 2008.
- [22] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science and Business Media, 2009.