Computer Science • 24(4) 2023 https://doi.org/10.7494/csci.2023.24.4.4986

Mamatha K R
Radhika K R

PROCESS OF FINGERPRINT AUTHENTICATION USING CANCELABLE BIOHASHED TEMPLATE

Abstract *Template protection using cancelable biometrics prevents data loss and hacking stored templates, by providing considerable privacy and security. Hashing and salting techniques are used to build resilient systems. Salted password method is employed to protect passwords against different types of attacks namely brute-force attack, dictionary attack, rainbow table attacks. Salting claims that random data can be added to input of hash function to ensure unique output. Hashing are speed bumps in an attacker's road to breach user's data. Research proposes a contemporary two factor authenticator called Biohashing. Biohashing procedure is implemented by recapitualted inner product over a pseudo random number generator key, as well as fingerprint features that are a network of minutiae. Cancelable template authentication used in fingerprint-based sales counter accelerates payment process. Fingerhash is code produced after applying biohashing on fingerprint. Fingerhash is a binary string procured by choosing individual bit of sign depending on a preset threshold. Experiment is carried using benchmark FVC 2002 DB1 dataset. Authentication accuracy is found to be nearly 97%. Results compared with state-of-art approaches finds promising.*

Keywords biohashing, cancelable biometrics, feature transformation, fingerprint

Citation Computer Science 24(4) 2023: 537–565

1. Introduction

Biometrics is a term that refers to an automatic identification or verification method that uses a person's behavioral or physiological features. Template protection technique depending on distance preserving hashing has captivated a lot of attention among all the current protection schemes because of its efficiency and simplicity in providing privacy preservation while archiving decent authentication performance.

Basic purpose of Biometric Template Protection (BTP) is to use a parameterized function to build a protected biometric template from an unprotected biometric template [20]. Hashing is one of the most used methods for constructing a BTP scheme. Biohashing and Locality Sensitive Hashing (LSH) are two primary varieties of distance-preserving hashing used for BTP.

Biohashing is the first attempt to use such a technique to biometrics for the purpose of preserving a human fingerprint template by Jin et al [8]. Biohashing has been used on a variety of biometric modalities including faces, fingerprints and palmprints by Kong et al [11] and Iris, human speech.

Sadhya et al designed a cancelable framework for Iris templates by utilizing a technique known as LSH which will generate Locality Sampled Code template from sample iris codes. LSH is most commonly used to minimize data dimensionality by accurately mapping comparable input into the same buckets. Cryptographic hashes try to lessen collision probability, whereas LSH focusses to maximize possibility of collision for related items. Experiment carried on CASIAv3 and IITD iris databases shows Equal Error Rate (EER) of 0.105% and 1.4% respectively.

Biometric-based authentication systems are widely used due to their ease of use in handling identities. However, as a result of widespread acceptance and deployment of biometric systems, concerns about security and privacy of biometric data have developed. Biometric data, for example, can lead to the revealing of sensitive personal information. Furthermore, because the compromised biometric data is permanently linked to the user's identity, it may not be cancelled. Many research attempts have been conducted in recent years to overcome the aforesaid difficulties, such as template protection techniques (BTP) such cancelable/revocable biometrics. Cancelable biometrics is a parameterized claimed irreversible, revocable transform that ensures the biometric template's security and privacy. New template for the same individual might be created using different transformation function values if altered biometric template's integrity is compromised.

Hatef Otroshi Shahreza et al utilized Biohashing algorithm to secure features extracted from finger vein templates [21]. Unprotected biometric template is indicated by T_1. User's key K_1 along with T_1 is used to generate protected template T_2 by biohashing algorithm.

During enrollment, user's key and biohash templates will be stored at system database. Probe template should be compared with template in database for verification stage. Hamming distance is computed between model template and probe

template to find similarity score. Experiment is carried on publicly accessible finger vein UTFVP dataset to generate protected templates of length varying between 30 to 1000.

User-device Physical Unclonable Function (UDPUF) Biohashing-based was presented by Zheng et al and is used to authenticate both device and user in a Bring Your Own Device (BYOD) system [27]. A physical unclonable function (PUF) is a physical thing that generates a physically determined digital fingerprint output (response) that serves as a unique identity for a certain input and conditions (challenge). Vast majority of PUFs are based on natural physical variations that occur during semiconductor production.

PUF is a physical entity contained in a physical building that is often built in integrated circuits and used in applications that require high security, such as encryption. UD PUF offers an intriguing way to link a biometric feature to a device's fingerprint in order to improve access control vigilance. Biohashing serves as a link between device and user's biometric data.

Facehashing, a form of Biohasing, is used on a feature vector derived from facial region to generate facecode F_1. Facehashing is performed using three tokens: two system dependent tokens, t_{g1} and t_{h1}, and one subject specific token, t_{s1}.

Existing facehashing technique can be described as given by equation 1:

$$g_{f1} * R \xrightarrow{ts1} Y_1 \xrightarrow{\{0,1\}} h_{f1} \tag{1}$$

where h_{f1} is cancelable FaceCode and g_{f1} is original feature vector R_0 is a random matrix generated using subject assigned token ts1. R_0 is normalized using Gram-Schmidt Orthogonalization method on each column of R_0 to obtain R.

Modified FaceHashing method is described as given by equation 2:

$$g_{f1} * R \xrightarrow{ts1} Y_1 \xrightarrow{\Pi_{t1}(Y_1)} Y_2 \xrightarrow{\Pi_{t2}(Y_2)} Y_3 \xrightarrow{s1} j_{f1} \tag{2}$$

Where $t_1 = t_{s1} + t_{f1}$, where t_{f1} is a system-assigned token that is shared by all subjects. A permutation function P generates Y_2 by applying it t_1 times to the elements of vector Y_1. Permutation function is applied to the elements of Y_1 to create the vector Y_3, with the token $t_2 = t_{s1} + t_{f2}$. Original face features are retained offline and the feature vector h_{f1} is used for online identification.

Biohashing-based template protection technique is described by Zhang et al [26]. New sampling approach named algorithm for generating binary sequences with a binary tree structure is introduced to construct a finger vein feature of fixed length coding to improve performance caused by user token leakage.

After N_1 rounds, number of binary tree levels is N_1. Biohash code Length, Len, composed by organizing a binary tree is indicated in expression below as equation 3:

$$\text{Len} = \sum_{i1=1}^{n1} HammingDist_{i1} \tag{3}$$

In each layer Finger vein coding weight developed is adaptively set during authentication step to compute Hamming distance. Following equation 4 depicts computation procedure:

$$\text{HammingDis} = \sum_{i1=1}^{n1} W_{i1} HammingDist_{i1} \tag{4}$$

Where n1 is layer count in a binary tree, w_{i1} is weight of $i1^{th}$ layer's feature coding and $HammingDist_{i1}$ is Hamming distance of $i1^{th}$ layer's coding. Hamming distance is a metric for comparing feature templates that need to be verified and registered.

Three desirable properties of cancelable biometrics such as Irreversibility, Diversity, unlinkability on images from our own dataset as presented in section 6.

Contribution of this research work is given as below:

- The number of sectors on fingerprint image is not specific in other papers. This is important to identify the reference point and region of interest. Average absolute deviation values are computed in each sector to compute fingercode.
- In the proposed work, the number of sectors is specific to 80,160,192,256,288 and 320.
- Noninvertible function is applied to biometric data. Updatable templates are obtained by modifying the parameters of applied transforms. Potential imposters cannot reconstruct the entire biometric data.

Section 2 describes various State-of-Art approaches. Cancelable biometrics for fingerprint by utilizing gabor filter and biohashing is presented in Section 3. Experiment details are explained in Section 4. Section 5 details Experiment and Results. Cancelable metrics to be observed in Section 6. Finally Conclusion and Future work is presented in Section 7.

2. State-of-art

Using Permuted Randomized Non-Negative Least Square (PR-NNLS) optimization, Kho et al. developed a minutia descriptor based on Partial Local Structure (PLS) and proposed a non-invertible transformation for the production of cancelable fingerprint templates [9]. PR-NNLS preparation is distinctive in that it uses a noninvertible transformation on PLS descriptor dictionary rather than minutiae descriptor, which is known to degrade performance. In terms of EER, an experiment conducted on five subgroups from FVC 2002 and 2004 showed higher performance. Cancellability, unlinkability, performance criteria and non-invertibility are all provided by this method.

Kim et al present FACT, a method based on keystroke dynamics approach in which authentication is depending on Free text, Accelerator, Co-ordinate and Time for mobile devices [10]. Participants gave keystroke data in both Korean and English

languages to examine consequence of typing language on KDA. Cramer-von Mises criterion and Kolmogorov Smirnov statistic are used to analyze two keystroke feature distributions. Results of 500 test keystrokes on Korean generated an EER of 0% on average. For free-KDA, FACT model, which is based on 17 micro behavioral variables including fingertip size, hand size, muscle flexibility and finger length, provides superior user authentication performance on mobile devices. Partial Discrete Wavelet Transform(DWT) and window shift XOR models are used to create alignment-free cancelable fingerprint templates with dual protection by Shahzad et al in [22]. Window shift XOR model defuses Attack Via Record Multiplicity threat and partial DWT is used to enhance matching performance.Evaluation on public databases such as FVC 2004 DB2, DB1 and FVC2002 DB3, DB2 and DB1 shows EER of 4.69%, 7.35%, 1.63%, 0% and 0%.

Novel single-template strategy that uses local stability-weighted dynamic time warping and mean templates to meet recent demands for automated security systems to simultaneously improve accuracy and speed of online signature verification is provided by Okawa et al in [18]. A time-series averaging technique known as Euclidean barycenter-based DTW barycenter averaging method isused to obtain an effective mean template set for each feature. Dissimilarity between test template and mean sample is computed using local stability-DTW distance. MYCT-100, SVC2004 Task2 and 3DAirSig datasets are used for experimentation show promising results in both random-forgery and skilled-forgery scenarios. Authentication of wearable users is performed using physiological (heart rate), behavioral (step count) and hybrid (metabolic equivalent of a task and calorie burn) forms of coarse-grained processed biometric data that are less revealing is done by Vhaduri et al [24]. Significant features are selected from NetHealth mobile crowd sensing dataset by Kolmogorov Smirnov test, followed by Pearson Correlation based approach and Standard Deviation based feature selection to reduce feature count are performed. Unary Gaussian SVM and Binary Quadratic SVM are used for classification on NetHealth data implies hybrid biometric show better performance over physiological or behavioral biometrics.

Chang et al propose a non-invertible, bit-wise encryption solution to overcome constraints of existing transformation technique [4]. Using first biometric template, a fuzzy extractor is utilised to produce a random string from two biometric data. Second transformation function turns a protected biometric template into a second biometric template. Bit-wise encryption is presented using two separate algorithms. Over a homomorphic encryption-based system, the time spent for enrolment beats both offered algorithms. The experiment, which used IITD Iris database and the XM2VTSDB Face database, took 30 milliseconds to complete authentication. Dynamic hand-gesture has huge potential value with advantage of template-replaceability and safety as suggested by Liu et al [15]. SCUT-DHGA is a vast Dynamic Hand Gesture Authentication dataset that contains over 1.86X1000000 frames in both depth and color modalities, as well as 29,160 dynamic hand gesture video sequences, all collected from 193 volunteers. Two types of authentication tasks are investigated using six different forms of dynamic hand gestures: gesture-free and gesture-

predefined authentication. On SCUT-DHGA dataset, Open-set approach produced best EER of 6.96% in a cross-session scenario and 0.77% in a single-session situation.

Table 1 describes various state-of-art cancelable biometric authentication methods. One Cycle Attack is proposed by Zhu et al as a means to circumvent existing gait authentication systems [28]. A multi-cycle Wavelet Packet Decomposition Long Short-Term Memory (WPD LSTM) defensive model is provided to enhance sensor-based gait authentication and counter-attack resistance. WPD LSTM model uses contextual information from surrounding gait cycles to determine gait sequence. It was discovered that hostile gait cycles formed using clustering method can quickly circumvent victim's model using six models: CNN+LSTM, LSTM, CNN, DTW, SVM, and PCC. Experiments on two datasets OU-ISIR and GREDO datasets, show that utilising imitation, a single cycle assault can compromise most of the victims in 5 attempts. When a multi-cycle defence mechanism is utilised, success rate of attackers is drastically lowered.

Jong Im et al demonstrated a mobile biometric authentication platform that supports for real-time computation of a Euclidean distance based matching function, maintaining safety from hostile clients and curious servers [7]. Real-time biometric authentication system with efficient squared Euclidean distance computation. Catalano-Fiore transformation is refined in order to obtain quadratic homomorphic encryption from linear homomorphic encryption, halving the computational difficulty of decrypting a quadratic ciphertext. Face processing and authentication are two software modules in a privacy-preserving face verification system. For face processing module, ResNet is used to generate a feature vector. An experiment using two public face datasets, ORL and CFP, yielded EER values of 0.37 percent and 1.17 percent, respectively. Secure face verification takes only 1.3 seconds on a smartphone.

Spectral transform-based approach proposed by Abdullahi et al utilizes a geometric transformation to extract a corresponding domain from minutiae, enabling building of a fixed-length representation of minutiae [1]. Using spectral transformations, Fourier Mellin creates a geometric transformation based on spectral minutiae. When Fourier-Mellin is utilized to translate fingerprint minutiae into a related domain, a good balance between discrimination and robustness is achieved. To ensure robustness, the minutiae set is represented via a fixed-length minutiae representation. Resulting minutiae representation is flattened using fractal coding to ensure compactness and efficient authentication. Contractive transformation is used in fractal coding to compress visual information to suit the self-similarity of an image. In a study including six FVC 2004 and FVC2002 databases, average transaction time was 1.3834 seconds.

Employing known sample attack for Biometric Template Protection schemes that uses distance-preserving hashing as demonstrated by Lai et al [13]. Most current template security techniques are shown to be vulnerable in a couple of seconds, especiallly when output sample size is much smaller than actual input sample size. Robust authentication system is introduced to combat such an attack.

Table 1
State-of-Art table

Author	**Method**	**Dataset**	**Biometric Performance (EER)**
kaur (2018)	log gabor filter, random distance method	CASIA-Face V5, IRIS, CASIA NIR, IRIS (LWIR), CASIA Palmprint, CASIS-MS V1(WHT), CASIA-MS V1(940), SDUMLA-HMT	2.60 ± 1.3, 2.68 ± 1.17, 0.80±0.23, 0.96±0.56, 0.53±0.21, 0.60±0.45, 0.99±0.21, 1.19±0.53
Kho (2019)	Permuted Randomized Non-Negative Least Square	FVC 2004 DB1, FVC 2002 DB4, DB3, DB2, DB1	4.51%, 5%, 3.61%, 0.06% and 0.01%
Vhaduri(2019)	Gaussian SVM and Quadratic SVM	NetHealth Crowd sensing Dataset	0.05%
Sadhya (2019)	Bit Sampling Based Locality Sensitive Hashing	IITD, CASIAv3	1.4%, 0.105%
Kim (2020)	Cramer-Von Mises criterion and Kolmogorov Smirnov	Proprietary dataset	0.45% for English language, 0.08% for Korean language
Chang (2020)	1D Log Gabor algorithm, Bloom filter and Bit-wise encryption	IITD Iris, CASIA Iris, XM2VTSDB Face	-
Im (2020)	Linear Homomorphic Encryption	CFP, ORL	1.17%, 0.37%
Lai (2021)	Randomized Locality Sensitive Hashing	LFW Face	0.98%
talreja (2020)	Bilinear Architecture, Fully Concatenated Architecture	WVU Multimodal 2012 face and Iris	1.99%, 1.45%
Abdullahi (2020)	Fourier Mellin Transform and Fractal Coding	FVC2004, FVC2002	2.348%, 0.364%
Shahzad (2021)	windows-shift-XOR, partial DWT	FVC2004 DB1, DB2, FVC2002 DB1, DB2, DB3	7.35%, 4.69%, 0%, 0%, 1.63%
Okawa (2021)	time series averaging method, local stability-weighted dynamic time warping	SVC 2004 Task2 / MYCT-100 online signature dataset, 3DAirSig	2.08%, 0.72%, 0%
liu (2021)	Feature Extraction Backbone and TIE module	SCUT-DHGA (Dynamic Hand Gesture Authentication Dataset)	0.77%
Zhu (2020)	Cycle extraction Algorithm along with adversarial gait cycle matching algorithm	OU-ISIR, GREDO	7.27%, 6.99%
tran (2021)	Encoded MCC, KNN Clustering algorithm	FVC 2004 DB2, FVC 2002 DB1, DB2, DB3	3.25%, 0.23%, 0.08%, 1.46%

Countermeasure for a distance-preserving transformation-based attack employs a locality sensitive hashing family constructed utilising a randomised approach to provide non-linearity for security goal. A LSH function has been reformulated to generate a fixed number of points that can be expressed directly in terms of number of stripes in hashed domain. Some deep learning methods such as deep neural networks have progressively been employed in vein recognition system [12].

3. Cancelable biometrics for fingerprint by utilizing gabor filter and biohashing

3.1. Preprocessing

I(p,q) represents intensity of pixel at p^{th} row and q^{th} column in a gray level fingerprint image. Variance and Mean of a grayscale fingerprint image, I, are calculated as in equations (5) and (6) respectively:

$$\text{Var(I)} = \frac{1}{N^2} \sum_{p=0}^{N-1} \sum_{q=0}^{N-1} (I(p,q) - M(I))^2 \tag{5}$$

$$\text{M(I)} = \frac{1}{N^2} \sum_{p=0}^{N-1} \sum_{q=0}^{N-1} I(p,q) \tag{6}$$

Reference point must be situated in same location in each impression of finger to acquire correct information. Following is how reference point detection technique works: To begin, fingerprint image is separated into 8x8 blocks. Following that, each block's gradient is computed and gradients are used to calculate an estimation of orientation field. Highest curvature of fingerprint ridges is defined as reference point. As a result, ridge curvature must be determined. O is an N × N orientation image in which O(p,q) shows local ridge orientation at each pixel (p,q). Rather than specifying local ridge orientation for each pixel, it is more common to provide it for a block. A separate ridge orientation is established for each of w × w non-overlapping blocks that make up an image.

Spatial tesselation of a fingerprint picture that includes a Region of Interest(ROI) is defined by a collection of sectors. Eight homocentric bands around focal spot is employed. Each band is divided into 10 sectors and measures 16 pixels wide. As a result, we get a total of 10 x 16 = 160 sectors, with a 100-pixel-radius circle centred at core point as region of interest.

Normalization is used to eliminate impacts of sensor noise and gray level backdrop caused by changes in finger pressure. Normalization is a pixel-by-pixel process as shown by equation 7 given below. Clarity of furrow and ridge structures is unaffected. Normalization's main goal is to reduce fluctuation in gray level values along furrows

and ridges, making following processing steps easier.

$$\mathrm{NI(p,q)} = \begin{cases} M_0 + \sqrt{(\frac{(V_0 \times (I_{p,q}) - M_i)^2}{V_i})} \;\; if \; I_{p,q} > M_i \\ M_0 - \sqrt{(\frac{(V_0 \times (I_{p,q}) - M_i)^2}{V_i})} \;\; Otherwise \end{cases} \tag{7}$$

where V_i and M_i are estimated variance and mean of gray levels in sector S_i respectively, V_0 and M_0 are desired variance and mean values, respectively.

3.2. Gabor filter

Gabor function are used to detect edges. Two-dimensional Gabor filter can achieve optimal localization in both frequency and spatial domains, allowing it to precisely characterise image local structural information such as spatial direction, spatial location and spatial scale selectivity. Gabor filter's direction and frequency representations are similar to those of human vision system and they're frequently employed to describe and represent texture characteristics. By using appropriately calibrated Gabor filters, true furrow and ridge structures of a fingerprint image can be dramatically enhanced. These emphasised furrow and ridge characteristics reflect a fingerprint impression well.

Fingerprint image is broken into eight component images using eight different values of K such as 0°, 22.5°, 45°,.... Fingerprint image I(p,q) is normalised and convolved with each of eight Gabor filters to create eight component images. Convolution with an orientated filter emphasises ridges that are parallel to x-axis while smoothing ridges that are not. Eight component images capture majority of ridge directionality information included in a fingerprint image and hence comprise a viable representation. Single set of values are provided for parameters of Gabor filter to obtain an approximate optimum response instead of optimum response for blood vessel segmentation in retinal images to achieve maximum Gabor filter response as by pratap et al [19]. Usage of lesser Gabor filters decreases a greater extent in processing time. Information technology of biometric identification based on gabor and log-gabor wavelets is presented by bychkov et al in [3].

2D Gabor filter equation in generalized form is given by equations 8 - 10.

$$h1(p,q;\psi,e) = exp\left(\frac{p_\psi^2}{\alpha_p^2} + \frac{q_\psi^2}{\alpha_q^2}\right) cos(2 \cdot \pi \cdot e \cdot x_\psi) \tag{8}$$

$$p_\psi = p \cdot sin\psi + q \cdot cos\psi \tag{9}$$

$$q_\psi = p \cdot cos\psi - q \cdot sin\psi \tag{10}$$

Where, ψ is Orientation of Gabor filter, 8 different values are considered such as 0° , 22.5°, 45°,..., α_p and α_q are shape constant of gaussian envelope along X and Y axes respectively, e is frequency of sinusoidal plane wave.

Fixed length feature vector is calculated by extracting global and local features of a fingerprint image. Thus Mean Absolute Deviation (MAD) of each 8×8 block of eight filtered images defines components of fingercode. is shown by equation (11)–(12).

$$Mean = \frac{1}{m}\sum_{r=1}^{m} s_r \tag{11}$$

$$Deviation = \sqrt{\sum_{r} E(p,q) - Mean} \tag{12}$$

where $E(p,q)$=Sector of Filter image and r=Number of pixels in Sector. MAD of each 8×8 block of eight filtered images defined components of fingercode.

Output of Gabor filter on sample fingerprint is shown in figure 1. Biocode generation on sample fingerprint is also shown in diagram.

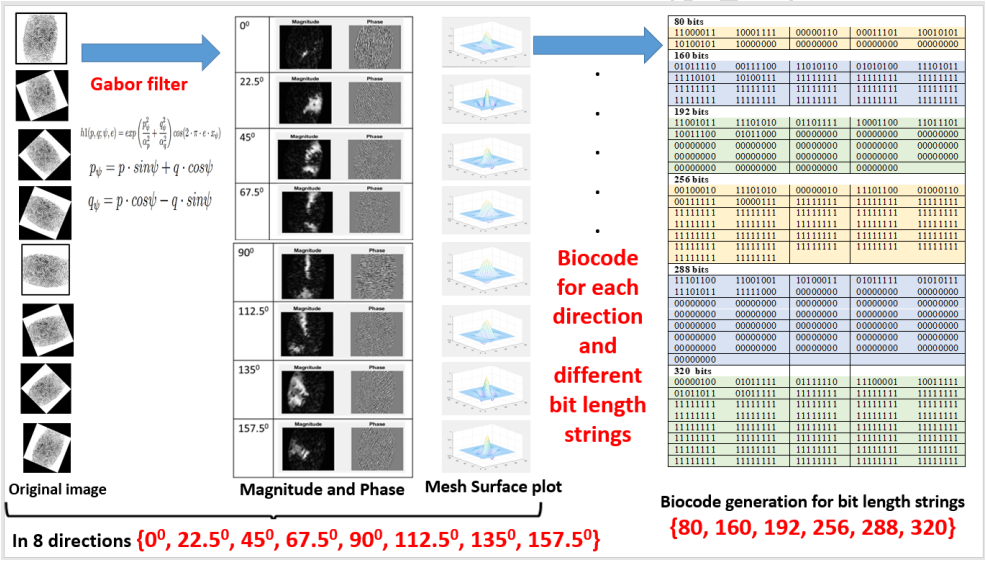


Figure 1. Summary of 2D gabor filter in Biohashing

3.3. Biohashing

Biohashing is first presented as a means of safeguarding biometric traits. Basic idea behind biohashing is to transform a raw biometric feature onto a new random space and save generated templates for subsequent processing. Modified templates and also transformation factors must be recorded. Transformation function must not be invertible and transformed results must retain intraclass distance.

Biohashing method has several advantages. Biohashing template has a high tolerance for data acquisition offsets, resulting in highly correlated bit strings (Biohashes)

when same biometric feature is acquired at various times. Biohashing technique solves problem of biometric features' irreversibility: If saved templates are compromised, user can easily change one-way transform function with a new one by enroling with a different secret seed or replacing token. Biohashing is amongst most widely employed biometric template protection mechanisms currently. Teoh et al proposed Biohashing. Biohashing has goal of producing a binary BioCode. Principle of BioCode formation employing Biohashing is shown in Figure 2.

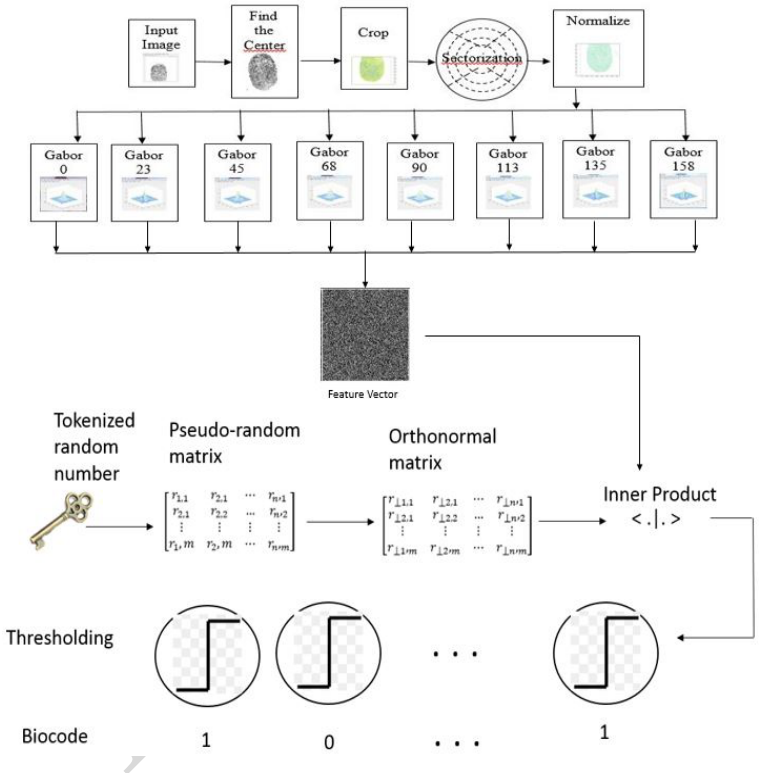


Figure 2. 2D gabor filter in Biohashing

Biometric data are combined with a tokenized random numbre (TRN) to generate BioCodes in Biohashing approach. This procedure is used during subject enrolment and verification. Upon enrolling, resulting BioCode is recorded and during subject authentication during verification, BioCode is recomputed. Biohashing approach minimizes dimension of original feature vector by using a random projection technique that is completed after extraction of biometric traits.

Suggested solution is unique in that it uses Biohashing to protect minutiae templates as in [2] and palm print and palm vein templates as in [5]. Biohashing is mathematically demonstrated to be non-invertible and highly cancelable.

Nanni and Lumini present a better Biohashing algorithm that uses random subspace to build K features [16]. Employing image-based features and a single point, biohashing concept is more appropriate to apply. Based on given metrics, A. Nagar investigated security of two well-known template transformation approaches, namely Biohashing and cancelable fingerprint templates, using specified metrics [17]. Teoh et al proposed Biohashing to protect biometric templates by employing Random Multispace Quantization (RMQ) [23].

Three techniques are used to preserve biometric data are : linear transformations such as Principal Component Analysis (PCA) and Fisher Discriminant Analysis (FDA), projection into multiple subspaces and quantization are three processes. In terms of performance, this strategy yields a small error rate. However, because fingerprint minutiae can change from capture to capture, it is irrelevant in fingerprint biometrics.

3.4. Proposed system

Algorithm 1 shows steps for Biocode generation using 2D Gabor filter and biohashing algorithm.

First step is to find core point for inputted fingerprint image. Numerous methods available in literature to find core point are Hierarchical method based on fingerprint gradient, using gradient and continuous vector field, Enhanced Gradient field based algorithm to obtain smoother field and so on. Spatial tessellation of fingerprint image which consists of region of interest is defined by a collection of sectors. Four concentric bands around core point are used. Each band is 20 pixels wide and segmented into thirty two sectors. Thus we have a total of 32 x 4 = 128 sectors and region of interest is a circle of radius 100 pixels, centered at core point.

Normalization is performed to remove the effects of sensor noise and gray level background due to finger pressure differences. Aim of normalization process is to standardize intensity values of a fingerprint image by adjusting gray level coverage to fall within expected value range. This process preserves clarity of ridge and valley structures while primarily reducing variation of gray values along them. Normalization enhances image contrast and brightness by ensuring that gray level values are limited to a certain range, making subsequent processing steps easier. Image normalization is a vital step in fingerprint analysis as it aims to improve quality of fingerprint images by enhancing contrast between ridges and valleys. Through standardization of intensity values, normalization helps to achieve this goal.

Gabor filters optimally capture both local orientation and frequency information from a fingerprint image. By tuning a Gabor filter to specific frequency and direction, local frequency and orientation information can be obtained. By combining sinusoidal and Gaussian components, Gabor filter method constructs a filter that effectively links ideal representation of orientation direction and spatial frequency domain. Gabor originally introduced the Gabor function in 1946, defining it in 1-D with "t" representing time and it was later extended to a 2-D function in spatial domain.

Algorithm 1: Two Dimentional gabor filter based biohashing algorithm for generation of Cancelable fingerprint

Inputs:

T_1: unprotected biometric template

L_1:length of unprotected template 388 X 374 (142KPixels)

L_2:length of protected template (80,160,192,256,288,320 bits)

k_1: user's seed.

Output:

$B = \{b_{i1}|i1 = 1, 2, ...m_1\}$ binary Biohash protected template

Pseudocode:

▷ Algorithm used to generate fingerhash code is given in pseudocode form here.

Used conspicuous landmakrs for locating reference point in fingerprint image T_1 whose length is L_1 and computed region of interest on 80 sectors.

Tessalation is done around reference point to find region of interest.

Normalization is performed to remove effects of gray level background and sensor noise due to finger pressure differences.

Filtering region of interest in 8 direction using 2D Gabor filters is performed. In generalized 2D Gabor filter equation 8 different values are considered such as 0° , 22.5°, 45°,... for extraction of features.

Obtained a n-bit feature vector by calculating MAD of gray values in several sectors of filtered picture known as T_2. Fingercode generating equations are given earlier.

Produce a pseudo-random vectors set,

$$r_i \in \{R^M|i = 1, 2, ...m_1\}$$

where $m_1 \ll n_1$ based on m that is length of final biohash value and user's seeed k_1.

Employ Gram-Schmidt process to convert pseudo-random vectors $\{r_i \in R^m|i = 1, 2, \ldots, m_1\}$ into an orthonormal set of matrices $\{r_\perp \in R|i = 1, 2, \ldots, m_1\}$.

Compute random projection of T_2 with $r_{\perp i}$: $\{X_i =< T2|r_{\perp i} >\in R^m|i = 1, 2, \ldots, m_1\}$ where $< .|. >$ indicates inner product operation

Binarize projection result to obtain Biohashing code B using below equation

$$\begin{aligned} b_{i1} &= 0 \ if X_i \ \leq t1 \\ &= 1 \ if \ X_i \ > t1 \end{aligned}$$

where $t1$ is threshold value.

Producce $B = \{b_{i1}|i1 = 1, 2, ...m_1\}$.

Produce and return protected template L_2 of length 80,160,192,256,288 and 320 bits.

A unique ridge and valley structure on the skin over the fingers forms fingerprints, which are the oldest and most widely recognized biometric trait possessed by all human beings. These ridges and valleys usually run parallel to each other and contain terminations known as bifurcations and ridge endings. Ridge structure exhibits diverse shapes, including high curvature, bifurcations, terminations, crossovers and other characteristics collectively referred to as singularities. Fingerprints acquire their distinctiveness from distribution of singularities at local level, which are referred to as minutiae. Minutiae are various ways in which ridges can be discontinuous, including sudden endings or terminations and splits into two ridges, known as bifurcations. These singularities can be categorized into three topologies: loop, delta, and whorl.

Fingerhashing is a variant of Biohashing to generate fingercode from feature vector extracted from fingerprint images.Using subject assigned token, the random number generator generates a random matrix which is normalized using Gram-schmidth orthogonalization method on each column. Then original feature vector from fingerprint is projected on each column of orthogonlaized matrix. Afterwards inner product is computed which is a vector containing real values. Elements of vector quantized by selecting a threshold to get fingerhash code. Fingerhash values lie between 0 & 1.

Privacy and Confidentiality of data, authenticity of data is achieved through Biohashing. Biohashing approach offers numerous advantages including ability to revoke BioCode by applying same process with a different random number. Additionally, it allows for generation of different BioCodes to authenticate user to different services from same biometric raw data(e.g., fingerprint).

4. Experiment details

Proposed algorithm is evaluated on fingerprint images taken from FVC 2002 DB1 database which contains 100 fingerprints with eight samples per subject, total 800 images are included in database. Sample images from database for first subject are shown in figure 3. Experiment is carried out using MATLAB r2020a. Fingercodes of length 80, 160, 192, 256, 288 & 320 bits are generated for fingers in database.

Figure 3. Sample fingerprints of first subject in FVC 2002 DB1 database

Totally 200 images are rejected from database because image quality was inadequate or reference point was situated in a corner of image, making it impossible to determine a suitable region of interest. Person1 and Person2 biocodes are shown in tables 2 and 3.

Table 2
Person1 Biocode

length of 80 bits				
11000011	10001111	00000110	00011101	10010101
10100101	10000000	00000000	00000000	00000000
length of 160 bits				
01011110	00111100	11010110	01010100	11101011
11110101	10100111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
length of 192 bits				
11001011	11101010	01101111	10001100	11011101
10011100	01011000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	
length of 256 bits				
00100010	11101010	00000010	11101100	01000110
00111111	10000111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111			
length of 288 bits				
11101100	11001001	10100011	01011111	01010111
11101011	11111000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000				
length of 320 bits				
00000100	01011111	01111110	11100001	100111111
01011011	01011111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111

Table 3
Person2 Biocode

length of 80 bits				
11000011	10001111	00000110	00011101	10010101
10100101	10000000	00000000	00000000	00000000
length of 160 bits				
10100001	11000011	00101001	10101011	00010100
00001010	01011000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
length of 192 bits				
11001011	11101010	01101111	10001100	11011101
10011100	01011000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	
length of 256 bits				
00100010	11101010	00000010	11101100	01000110
00111111	10000111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111			
length of 288 bits				
11101100	11001001	10100011	01011111	01010111
11101011	11111000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000000				
length of 320 bits				
00000100	01011111	01111110	11100001	100111111
01011011	01011111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111

Each fingerprint snapshot in database is matched with all other fingerprints in database to ensure verification accuracy of fingerprint representation and matching

approach. In experiment [25], two different protocols (1 vs. 1 protocol and original FVC protocol) are applied.

Initial image of each subject is compared to first image of remaining subjects for imposter comparison in one vs. one protocol. For genuine comparison, first and second images of same subject are compared. 4950 imposter and 100 genuine comparisons are computed for 1 vs. 1 protocol.

Imposter comparison process is same as one vs. one protocol in original FVC protocol. Genuine comparison is done for each image of a subject with the remaining images of same subject. 4950 imposter and 1500 genuine scores are generated in original FVC protocol.

Four different proximity measures used in experiment are Cosine, Euclidean, Jaccard and Hamming computed using equations (13)–(16). Genuine and imposter distributions for four distances are shown in figure 4 to 7.

Four possible outcomes of a biometric system in verification mode are :

1. genuine rejection
2. imposter rejection
3. genuine acceptance
4. imposter acceptance

Second and third outcomes are correct, but fourth and first are incorrect. A biometric system's performance is measured in terms of False Accept Rate (FAR) and False Reject Rate (FRR). A trade-off exists between two sorts of faults. Genuine rejection rate is lower but FAR may be higher if a higher threshold is chosen and vice versa. Genuine acceptance rate is percentage of times system successfully detects two fingerprints representing same finger given a matching distance criterion.

FAR, on other hand, is percentage of times the system wrongly recognizes two fingerprints as belonging to same finger. FAR and FRR criteria are dictated by biometric application. A small FAR is required for entrance to a military base, whereas a small FRR is required for access to an ATM machine. Cosine similarity is given by equation (13).

$$\text{Cosine Similarity(A, B)} = \frac{A \cdot B}{||A|| \times ||B||} \tag{13}$$

Euclidean distance formula gives distance between two points (or) straight line distance. Let us assume that (A1,B1) and (A2,B2) are two points in a two-dimensional plane. Here is the Euclidean distance formula given in equation 14.

$$\text{Euclidean Distance(A, B)} = \sqrt{\sum_{i=1}^{k} (A_i - B_i)^2} \tag{14}$$

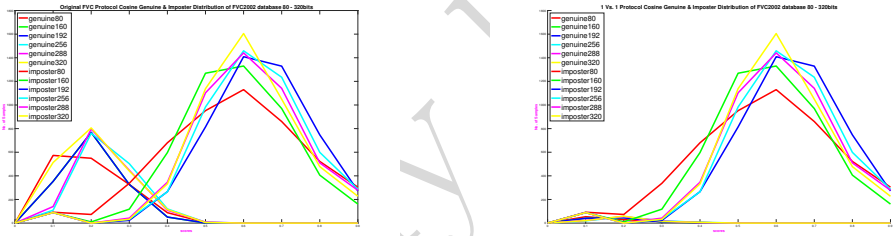
Jaccard Index, also known as Jaccard Similarity coefficient, is a statistic used in understanding similarities between sample sets is given by equation (15). Measurement emphasizes similarity between finite sample sets and is formally defined as size

of intersection divided by size of union of sample sets.

$$\text{Jaccard Index(A, B)} = \frac{|A \cap B|}{|A \cup B|} \tag{15}$$

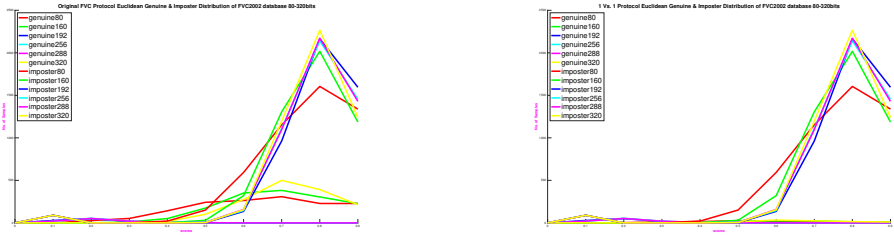
Hamming distance between two integers is number of bits that are different at the same position in both numbers computed using equation 16.

$$\text{Hamming Distance(A, B)} = \sum_{i=1}^{k} |A_i - B_i| \tag{16}$$



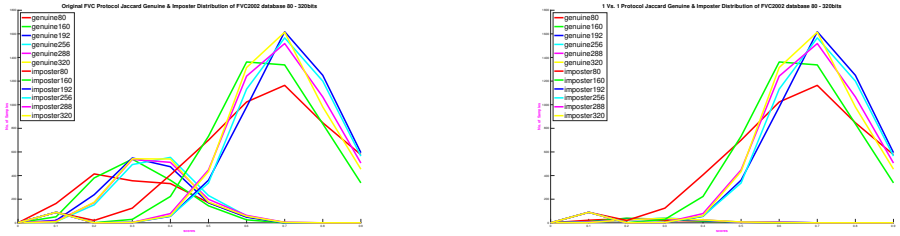
(a) (b)

Figure 4. Cosine Similarity



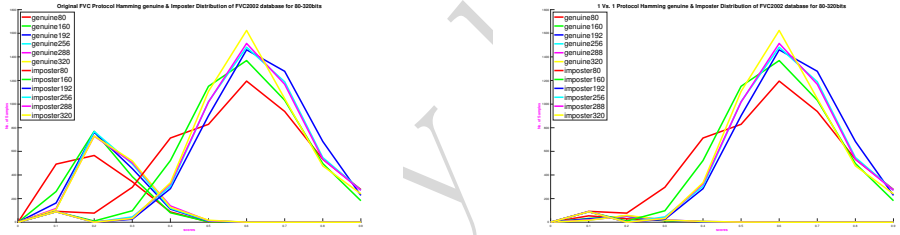
(a) (b)

Figure 5. Euclidean Distance



(a) (b)

Figure 6. Jaccard Index



(a) (b)

Figure 7. Hamming Distance

Separability calculated using equation 17 is shown in tables 4 and 5 to measure relation between genuine and imposter distributions. According to separability, Euclidean distance is best for fingercode of 320 bits for original FVC protocol and fingercode of 192 to 320 bits for 1 Vs. 1 protocol.

$$\text{Separability} = \frac{|\mu_{Ge} - \mu_{Im}|}{\sqrt{\sigma_{Ge}^2 + \sigma_{Im}^2/2}} \tag{17}$$

where μ_{Ge}, μ_{Im}, σ_{Ge} and σ_{Im} are mean and variance of genuine and imposter distributions.

Table 4
Separability (%) comparison for original FVC protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	0.0026	0.0029	0.0028	0.0012
160	0.0017	0.0017	0.0018	9.052e-04
192	0.0014	0.0016	0.0016	0.0011
256	0.0014	0.0016	0.0016	0.0011
288	0.0014	0.0016	0.0016	0.0011
320	0.0014	0.0013	0.0015	7.7100e-04

Table 5
Separability (%) comparison for 1 vs. 1 protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	0.0037	0.0043	0.0041	0.0017
160	0.0024	0.0025	0.0026	0.0013
192	0.0019	0.0014	0.0023	0.0011
256	0.0019	0.0023	0.0023	0.0011
288	0.0021	0.0024	0.0023	0.0011
320	0.0904	0.0021	0.00231	0.0011

5. Experiment and results

Evaluation metrics used in experiment are Precision, F-Measure and Accuracy calculated using equations (18)–(20) are shown in tables 6–11.

According to Accuracy, fingercode length of 288 bits is best choice for cosine distance metrics in original FVC protocol and 192 bits fingercode is best for 1 Vs. 1 protocol for jaccard and cosine similarity matrix.

$$\text{Precision} = \frac{\text{trP}}{\text{trP} + \text{faP}} \tag{18}$$

where trP stands for True Positives and trN stands for True Negatives.

Model's precision is number of fingerprint that were correctly authenticated, divided by all fingerprints that the model picked.

Table 6
Precision (%) comparison for 1 vs. 1 protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	4.7628e-04	3.3226e-04	3.4122e-04	8.1293e-04
160	3.8087 e-04	2.5784e-04	2.7313 e-04	7.4206 e-04
192	4.0967 e-04	2.8496e-04	3.1560 e-04	7.6776 e-04
256	4.1877 e-04	2.9488e-04	3.0213 e-04	7.5870 e-04
288	4.8413 e-04	3.5189e-04	3.7485 e-04	8.1272 e-04
320	4.7766e-04	2.7307e-04	3.6589 e-04	7.8907e-04

Table 7
Precision (%) comparison for original FVC protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	2.3e-03	1.4e-03	1.3e-03	5.9e-03
160	1.9e-03	1.1e-03	1.3e-03	6.1e-03
192	1.1e-03	6.3827e-04	6.9953e-04	4.4e-03
256	2.3e-03	1.4e-03	1.3e-03	5.9e-03
288	2.0e-03	1.2e-03	1.3e-03	5.9e-03
320	2.3e-03	1.4e-03	1.5e-03	6.0e-03

$$\text{F-Measure} = \frac{2 \text{ x Precision x Recall}}{\text{Precision + Recall}} \tag{19}$$

F-Measure is a way of combining precision and recall of model and it is defined as harmonic mean of model's precision and recall calculated using equation 19. F-Measure for 1 vs 1 protocol is shown in table 8 and original FVC protocol is shown in table 9.

Table 8
F-Measure (%) comparison for 1 vs. 1 protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	9.5165e-04	6.6409e-04	6.8198e-04	1.6 e-03
160	7.6115 e-04	5.1542e-04	5.4597 e-04	1.5 e-03
192	8.1868 e-04	5.6960e-04	6.3081 e-04	1.5 e-03
256	8.3684 e-04	5.8941e-04	6.0390 e-04	1.5 e-03
288	9.6732 e-04	7.0329e-04	7.4913 e-04	1.6 e-03
320	9.5442 e-04	5.4583e-04	7.3125 e-04	1.6 e-03

Table 9
F-Measure (%) comparison for original FVC protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	0.0045	0.0014	0.0026	0.0117
160	0.0038	0.0011	0.0025	0.0121
192	0.0022	0.0006	0.0014	0.0087
256	0.0045	0.0014	0.0026	0.0116
288	0.0040	0.0012	0.0025	0.0117
320	0.0046	0.0014	0.0029	0.0118

$$\text{Accuracy} = \frac{\text{trP} + \text{trN}}{\text{Total}} \tag{20}$$

where trP stands for True Positives and trN stands for True Negatives.

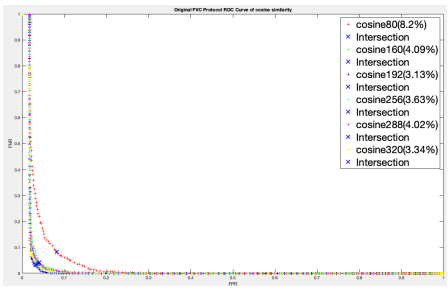
Table 10
Accuracy (%) comparison for original FVC protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	69.31	68.34	69.14	69.56
160	70.10	70.15	70.05	69.96
192	70.37	70.51	70.49	70.19
256	70.13	70.18	70.10	70.01
288	70.59	70.77	70.59	70.25
320	70.20	62.12	70.31	70.11

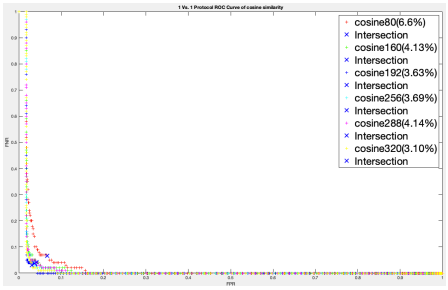
Table 11
Accuracy (%) comparison for 1 vs. 1 protocol

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	97.83	97.81	97.80	97.85
160	97.82	97.79	97.78	97.85
192	97.93	97.93	97.91	97.92
256	97.82	97.80	97.77	97.85
288	97.88	97.86	97.85	97.89
320	97.80	97.77	97.77	97.85

Receiver Operating Characteristic (ROC) curve measures overall system performance by plotting Genuine Acceptance Rate against False Acceptance Rate for all conceivable operating locations. ROC curves for all four distance measures are demonstrated as in figure 15–18.

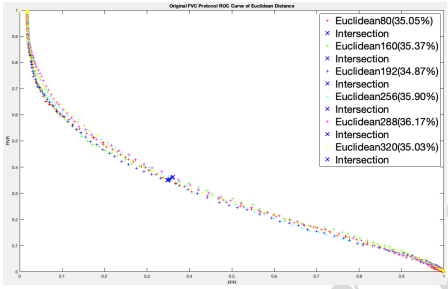


(a)

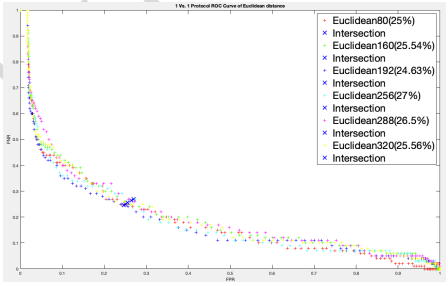


(b)

Figure 15. Cosine Similarity

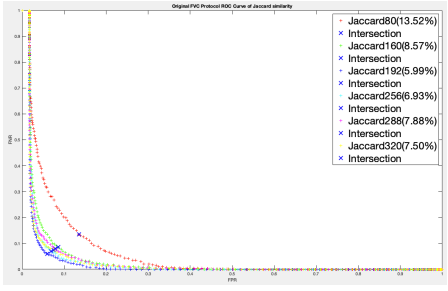


(a)

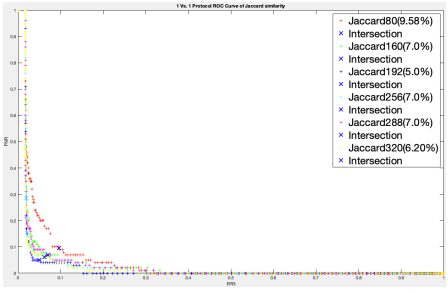


(b)

Figure 16. Euclidean Distance

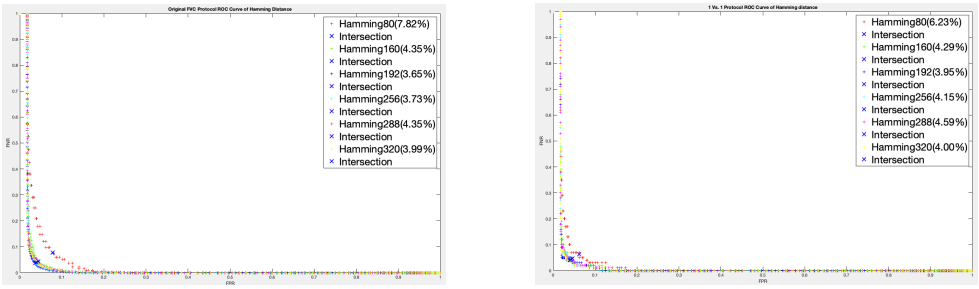


(a)



(b)

Figure 17. Jaccard Index



(a) (b)

Figure 18. Hamming Distance

According to Equal Error Rate(EER), 192 bits fingercode is best choice for original FVC protocol of cosine similarity and same length fingercode 1 Vs. 1 protocol of Jaccard similarity. Results of ROC curves is summarized in tables 12 and 13.

Table 12
Equal Error Rate (%) comparison for original FVC protocol (EER)

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	13.52	8.22	7.82	35.05
160	8.57	4.09	4.35	35.37
192	5.99	3.13	3.65	34.87
256	6.93	3.63	3.77	35.90
288	7.88	4.02	4.35	36.17
320	7.50	3.33	3.99	35.03

Table 13
Equal Error Rate (%) comparison for 1 vs. 1 protocol (EER)

No. of Bits	Jaccard(%)	Cosine (%)	Hamming(%)	Euclidean(%)
80	9.58	6.66	6.23	25
160	7.00	4.13	4.29	25.54
192	5.00	3.63	3.95	24.63
256	7.00	3.69	4.15	27.00
288	7.00	4.14	4.59	26.50
320	6.20	3.10	4.00	25.56

Result of experiment is compared with other techniques in the literature as shown in table 14.

Table 14
comparison with other techniques

Method	EER
Locality Sensitive Hashing by sadhya et al [20]	0.19%
Partial local structure by Kho et al [9]	0.01%
fractal coding and fourier mellin transform by abdullahi et al [1]	0.364%
one permutation Hashing by Li et al [14]	0.19%
Integer wavelet transform by Hashad et al [6]	0%
proposed	3.13%

Novelty of this paper: As per authors knowledge, it is first attempt in which Biohashing in fingerprint is applied on different lengths like 80 bits to 320 bits and four different distance methods are applied to compare FingerHash Codes like Hamming distance, Euclidean distance, Jaccard similarity and Cosine similarity. Rigorous study of biohashing on fingerprint biometrics applied to obtain cancelable fingerprint.

6. Cancelable metrics to be observed

Biohashing technique solves problem of biometric features irreversibility: If a user's saved templates are hacked, he or she can quickly switch to a new one-way transform function by enrolling with a different secret seed or replacing token. New dataset is created at our research centre comprising of 10 subjects. Pseudo-imposter and imposter scores on subject1 and subject4 proves Irreversibility. Diversity is ensured by choice of different functions for each application on subject2 and subject8. Unlinkability analysis is employed on generated dataset through mated and non-mated score distributions for subject3 and subject5.

Cancelability power of experiment: New fingerhash code can be generated if there is a leakage of fingerhash code by changing key used in biohashing procedure to provide cancelability.

7. Conclusion and future work

FVC2002 benchmark DB1 consisting of 6 out of 8 fingerprints for 100 individuals is considered. Fingercode of each user is generated following method presented in section, with a Gabor filter bank. Once this is achieved, 6 fingercodes are available for each person, which means 600 fingercodes of length 80 to 320 bits. After random projection and quantization, 600 BioCodes are issued. Unique columns from biocodes are selected for each subject which forms cancelable fingerhash code. Subject1 and subject2 fingerhash code is shown in table 15 and 16.

Table 15
Fingerhash code of Jaccard and Hamming distance for subject1

80 bits	15	22	37	41	58	64
160 bits	2	20	49	54	64	85
192 bits	9	25	33	45	58	61
256 bits	9	30	44	77	81	88
288 bits	19	83	89	118	139	142
320 bits	30	47	58	92	101	117

Table 16
Fingerhash code of Jaccard and Hamming distance for subject2

80 bits	8	9	27	45	54	63
160 bits	2	21	50	59	68	96
192 bits	3	7	11	19	25	50
256 bits	9	35	44	54	75	123
288 bits	9	19	27	35	75	88
320 bits	2	13	38	52	70	141

Fingercode is not cancelable since it uses raw fingerprint data. Obtained score is measured with Hamming, Jaccard, Cosine and Euclidean distance between the fingerprint kept as a reference and other fingerprints of database. Performance of a cancelable biometric system is evaluated with respect to BioCode. Some of the applications like Aadhar card, PAN Number, Retails sales counter etc can make use of this cancelable biometric method for privacy and authentication.

Irreversibility, Revocability, Diversity factors enhancement techniques for benchmark datasets are composed to future work.

References

[1] Abdullahi S.M., Wang H., Li T.: Fractal Coding-Based Robust and Alignment-Free Fingerprint Image Hashing, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2587–2601, 2020. doi: 10.1109/TIFS.2020.2971142.

[2] Belguechi R., Rosenberger C., Ait-Aoudia S.: Biohashing for Securing Minutiae Template. In: *2010 20th International Conference on Pattern Recognition*, pp. 1168–1171, 2010. doi: 10.1109/ICPR.2010.292.

[3] Bychkov O., Merkulova K., Zhabska Y.: Information Technology of Person?s Identification by Photo Portrait. In: *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, pp. 786–790, 2020. doi: 10.1109/TCSET49122.2020.235542.

[4] Chang D., Garg S., Hasan M., Mishra S.: Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3152–3167, 2020. doi: 10.1109/TIFS.2020.2983250.

[5] Fuksis R., Kadikis A., Greitans M.: Biohashing and Fusion of Palmprint and Palm Vein Biometric Data. In: *2011 International Conference on Hand-Based Biometrics*, pp. 1–6, 2011. doi: 10.1109/ICHB.2011.6094334.

[6] Hashad F.G., Zahran O., El-Rabaie S., Elashry I.F., Elbanby G., Dessouky M.I., El-Samie A., Fathi E.: Cancelable Fingerprint Recognition based on Encrypted Convolution Kernel in Different Domains, *Menoufia Journal of Electronic Engineering Research*, vol. 29(2), pp. 133–142, 2020. doi: 10.21608/mjeer.2020.103957.

[7] Im J.H., Jeon S.Y., Lee M.K.: Practical Privacy-Preserving Face Authentication for Smartphones Secure Against Malicious Clients, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2386–2401, 2020. doi: 10.1109/TIFS.2020.2969513.

[8] Jin A.T.B., Ling D.N.C., Goh A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number, *Pattern Recognition*, vol. 37(11), pp. 2245–2255, 2004. doi: 10.1016/j.patcog.2004.04.011.

[9] Kho J.B., Kim J., Kim I.J., Teoh A.B.: Cancelable fingerprint template design with randomized non-negative least squares, *Pattern Recognition*, vol. 91, pp. 245–260, 2019. doi: 10.1016/j.patcog.2019.01.039.

[10] Kim J., Kang P.: Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features, *Pattern Recognition*, vol. 108, p. 107556, 2020. doi: 10.1016/j.patcog.2020.107556.

[11] Kong A., Cheung K.H., Zhang D., Kamel M., You J.: An analysis of BioHashing and its variants, *Pattern Recognition*, vol. 39(7), pp. 1359–1368, 2006. doi: 10.1016/j.patcog.2005.10.025.

[12] Kuzu R.S., Piciucco E., Maiorana E., Campisi P.: On-the-Fly Finger-Vein-Based Biometric Recognition Using Deep Neural Networks, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2641–2654, 2020. doi: 10.1109/TIFS.2020.2971144.

[13] Lai Y., Jin Z., Wong K., Tistarelli M.: Efficient Known-Sample Attack for Distance-Preserving Hashing Biometric Template Protection Schemes, *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3170–3185, 2021. doi: 10.1109/TIFS.2021.3073802.

[14] Li Y., Zhao H., Cao Z., Liu E., Pang L.: Compact and Cancelable Fingerprint Binary Codes Generation via One Permutation Hashing, *IEEE Signal Processing Letters*, vol. 28, pp. 738–742, 2021. doi: 10.1109/LSP.2021.3071262.

[15] Liu C., Yang Y., Liu X., Fang L., Kang W.: Dynamic-Hand-Gesture Authentication Dataset and Benchmark, *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1550–1562, 2021. doi: 10.1109/TIFS.2020.3036218.

[16] Lumini A., Nanni L.: An improved BioHashing for human authentication, *Pattern Recognition*, vol. 40(3), pp. 1057–1065, 2007. doi: 10.1016/j.patcog.2006.05.030.

[17] Nagar A., Nandakumar K., Jain A.K.: Biometric template transformation: a security analysis. In: *Media Forensics and Security II*, vol. 7541, p. 75410O, International Society for Optics and Photonics, 2010. doi: 10.1117/12.839976.

[18] Okawa M.: Time-series averaging and local stability-weighted dynamic time warping for online signature verification, *Pattern Recognition*, vol. 112, p. 107699, 2021. doi: 10.1016/j.patcog.2020.107699.

[19] Pratap T., Kokil P.: Approximate Optimization of Gabor Filter Parameters in Application to Blood Vessel Segmentation in Retinal Images. In: *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, pp. 1–5, 2019. doi: 10.1109/WIECON-ECE48653.2019.9019964.

[20] Sadhya D., Akhtar Z., Dasgupta D.: A Locality Sensitive Hashing Based Approach for Generating Cancelable Fingerprints. In: *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–9, 2019. doi: 10.1109/BTAS46853.2019.9185991.

[21] Shahreza H.O., Marcel S.: Towards Protecting and Enhancing Vascular Biometric Recognition Methods via Biohashing and Deep Neural Networks, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3(3), pp. 394–404, 2021. doi: 10.1109/TBIOM.2021.3076444.

[22] Shahzad M., Wang S., Deng G., Yang W.: Alignment-free cancelable fingerprint templates with dual protection, *Pattern Recognition*, vol. 111, p. 107735, 2021. doi: 10.1016/j.patcog.2020.107735.

[23] Teoh A.B., Ngo D.C.: Cancellable biometerics featuring with tokenised random number, *Pattern Recognition Letters*, vol. 26(10), pp. 1454–1460, 2005. doi: 10.1016/j.patrec.2004.11.021.

[24] Vhaduri S., Poellabauer C.: Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users, *IEEE Transactions on Information Forensics and Security*, vol. 14(12), pp. 3116–3125, 2019. doi: 10.1109/TIFS.2019.2911170.

[25] Wang S., Hu J.: A blind system identification approach to cancelable fingerprint templates, *Pattern Recognition*, vol. 54, pp. 14–22, 2016. doi: 10.1016/j.patcog.2016.01.001.

[26] Zhang J., Fang P.: Finger Vein Template Encryption Scheme Based on BioHashing. In: *2018 International Conference on Sensing,Diagnostics, Prognostics, and Control (SDPC)*, pp. 681–685, 2018. doi: 10.1109/SDPC.2018.8664820.

[27] Zheng Y., Cao Y., Chang C.H.: Facial biohashing based user-device physical unclonable function for bring your own device security. In: *2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, 2018. doi: 10.1109/ICCE.2018.8326074.

[28] Zhu T., Fu L., Liu Q., Lin Z., Chen Y., Chen T.: One Cycle Attack: Fool Sensor-Based Personal Gait Authentication With Clustering, *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 553–568, 2021. doi: 10.1109/TIFS.2020.3016819.

Affiliations

Mamatha K R
B.M.S. College of Engineering, Visvesvaraya Technological University, Bangalore, krm.ise@bmsce.ac.in

Radhika K R
B.M.S. College of Engineering, Visvesvaraya Technological University, Bangalore, rkr.ise@bmsce.ac.in

Received: 01.09.2022
Revised: 24.10.2023
Accepted: 27.10.2023