TEMPLATE CONSERVATION METHODOLOGIES FOR MULTI-MODAL BIOMETRIC WITH LSTM NEURAL NETWORK

B.Nithya

Research Scholar, Department of Computer Science,
VISTAS, Pallavaram, Chennai,600043, India
nithya.phd@velsuniv.ac.in

P.Sripriya

Professor, Department of Computer Application,
VISTAS, Pallavaram, Chennai,600043, India
sri.scs@velsuniv.ac.in.

Abstract

In this work, we present a privacy-preserving multi-modal biometric system that uses LSTM (Long Short-Term Memory) neural networks for classification. Feature-level fusion has been applied over the features extracted by computer vision algorithms such as SURF (Speeded up Robust Features) and HoG (Histogram of Oriented Gradients). This work proposes two template preservation methods, bio-hash, and simple hash, to develop a secure architecture. The cancelability of the templates can be achieved by modifying the seed value of the random matrix. In the experimentation, various feature counts and their performances are tabulated under various metrics. The results show that when HoG feature method is applied, bio-hash method gives the lowest EER (Equal Error Rate) as 0.45 at feature count 10. And the simple hashing method's lowest EER is 0.34 at the feature count 10. When SURF feature method is applied, bio-hash method gives EER as 0.58 at feature count 30. And for simple hashing method, the lowest EER is 0.4 at the feature count 40.

Keywords: **Multi-modal Biometrics; LSTM; SURF; HoG; Cancelability.**

1. Introduction

Establishing the identity of a person by combining various body traits as evidence is known as a multi-modal biometric identification system [Jain A.K *et.al* (2008)]. These types of applications have the integration of a variety of biometric combinations to reach a successful identification system. The integration is in the form of multiple biometrics, multiple algorithms, multiple sensors, multiple images of same biometric signature or multiple parts of same trait [Clifton L. Smith *et.al* (2013)]. The evidence can be incorporated at different stages in a multi-modal biometric design that is referred to as fusion. Fusion of biometric signatures could be done before the matching process or after the matchers have given the match results. Feature vectors of the different biometric signatures can be fused and this can be simply done by concatenation of feature vectors. Fusion at feature level is considered to be an effective method since it has richer information [Zhao, W *et.al.* (2006)]. Using multiple modals of biometric in authentication system has several benefits over uni-modal biometric systems such as reduction in the rate of false non-matching (FNM) and false matching and also it prevents spoofing attacks [Kumar *et.al.* (2019)]. Even the multi-modal system has advantages over the single-factor, it will be affected by privacy risks due to widespread usage and data share. Attacks on biometric template databases are the most potential damage to the biometric system. These types of attacks are the route for the following three weaknesses. i) A stored template can be replaced by an unauthorized user's template, to get access to the system. ii) Entering into the authorized environment with a physical spoof that has been created using the stored template. iii) By having the template, a matcher can be compromised. The solution is to choose template preserving techniques and it is simply narrated as construction of cryptographic security on raw feature vectors [Toli*et.al.* (2004)]. To create a secured biometric authentication system, it must possess the below benchmarks:

i) Diversity: For ensuring user's privacy, unique templates must be created and database cross-matching should not be allowed.

ii) Revocability: If templates are compromised, a new template has to be reissued for the same biometric signature.

iii) Security: This criterion ensures that original templates cannot be obtained from the alternate template. It should prevent from spoofing attacks.

iv) Performance: If template security is given, the biometric system's performance should not be degraded.

The significant work in designing a biometric recognition system has to fulfill all the four requirements. The template protection schemes mainly classified into two categories, namely, cryptosystem and feature transformation. In cryptosystem [Y. H. Dandawate*et.al* (2015)], the biometric features are not stored as it. Instead of storing original features, the cryptographic key is generated using helper data from the biometric features. This method is further classified as key generation and key binding according to the usage of helper data. Salting/bio-hashing [Teoh*et.al* (2008)], non-invertible transformation[I. Raghu *et.al.* (2014)], key-binding [N. Lalithamani *et.al* (2009)], key-generating are various template protection techniques. In this paper, two template preservation techniques are used to create a multi-modal biometric authentication system, they are salting and hashing. In bio-hashing, the raw features are transformed into new feature space with the help of user-specific key. The key has to be saved securely and the user has to remember it. The hashing [K, Krishna *et.al* (2017)] method uses a key to generate hash code of raw features. The performances of these two techniques are verified on three biometric traits, fingerprint, face and signature. Our contributions in this work are as follows:

1. We suggest a multi-modal recognition with privacy preservation method based on SURF and HoG feature extracting algorithms.
2. We propose a LSTM (Long Short-Term Memory) based neural network classification to improve the performance.
3. We present bio-hashing and simple hashing privacy preservation method over biometrics trait's unique information on different feature counts in terms of accuracy, sensitivity, specificity, f-score, and EER (Equal Error Rate).

This work is arranged as follows, section 2 is about the literature review, the proposed work is described in section 3. Section 4 narrates results and the conclusion has been given in section 5.

2. Related

Various research works have been carried out on protecting biometric templates such as [6], [7], [9], [8], and [10]. In our work, the main focus is on two methods of protection. 1) Bio-hash and 2) Hash code protection. The authors [Lin You *et al.* (2008)] provided a multi-modal recognition based on a bio-hash protection. The authors fused the features and used a bloom filter to ensure that this random projection method increases the EER to 0.79. The writers [Padma polash paul *et.al.* (2015)] generates the random matrix according to the seed value for the orthogonal transformation of randomly fused raw features of face and ear. Performances are calculated using K-NN classifiers.[Keshav Gupta *et.al.* (2021)] is based on bio-hashed template protection and it was tested on various attacks' resistance such as brute-force, attacks via multiplicity, blended substitution attacks. The researchers in this work brought the EER value to 0.004 by using the bio-hash and they have concluded that they have received the most promising results with the proposed method. [HarkeeratKaur *et.al.* (2019)] proposed a multi-modal revocable biometric by combining face, thermal face, palmprint, palm-vein, and fingervein. Log-gabor filters method gives discriminant features and templates are transformed using random distance privacy-preserving technique. In this work, the feature dimension has been reduced automatically by 50%.[Abdellatef, E *et.al.* (2020)] extracted unique features with multiple CNN (Convolutional Neural Network) architecture and the concatenation of biometric features is done at the internal CNN layers. Security and privacy are maintained by bio-convolving without reducing the recognition accuracy. The main disadvantage of this work is time consuming due to the extra work of bio-convolving. [Rima Belguechi *et al.*(2017)] give bio-hashing protection based on texture. The main objective of this work focused on the robustness and security of cancelable template preservation. The performance is calculated based on EER value on various attacks over bio-hashing such as brute-force, stolen token, and attack by eavesdropping. They found that stolen token reaches severe attack with 0.28%. [Bedad Fatima *et al.* (2018)] presented bio-hash template protection over uni-modal with 0% of EER by combining various sensors. The bio-hash method is used by many researchers and they have given better recognition results with uni-modal as well as multi-modal. The hashing method of protection is chosen by [Aithal*et.al* (2017)] with 32-bit MD5 hash code generation of the fingerprint. This work concentrated on Euclidean distance calculation of fingerprint binary image before hash code generation. The calculated hash code is non-invertible and it consumes little amount of memory but this proposed system is not compatible if the different orientation of the same fingerprint is obtained. To create cancelable fingerprint minutiae, symmetric hash functions [Tulyakov*et.al.* (2005)] are created for each minutia and a corresponding matching algorithm is also constructed. This work overcomes the issue of differences in hash codes between enrollment and verification by matching minutiae of a localized set but it achieved a lower accuracy rate than plain-match of fingerprints. [Veeru Talreja *et.al.* (2019)] selected CNN classification layers to authenticate a person with multi-biometric instead of using a conventional matching algorithm. This proposed scheme has multimodal deep hashing module for creating binary hash code from the sign activation function at different layers in CNN architecture. Error-correcting code is adopted to face the issue of the differences in hash codes between enrollment and probe image. A hash function is also used for creating a biometric password using the traits. [Aravind Ashok *et.al.*(2012)] proposed a biometric protection technique with a cryptographic hash method of Secured Hash Algorithm (SHA). But the authors failed to discuss about the matching and recognition performance of the proposed system. [Zhe Jin *et al.*(2018)] generated cancelable templates using Index-of-Maxing (IoM) technique that is based on ranking and locality sensitive hashing. Fingerprint biometric minutiae and its orientations are extracted to apply the proposed method. The main focus is on finding maximum index value of the feature vector and hashing the selected value. The researchers prove that this work is strongly resists on various attacks such as brute-force, false-accept attack, attacks via multiplicity and birthday attack. From the literature review, the research gap has been identified that signature image has not considered most for authentication. And the hash code generation method is less chosen by the researchers in multi-modal system. Our work takes three modalities, fingerprint, face and signature to make secure multi-modal system. Also at the matching phase, this effort chooses neural network idea for automatic classification through learning the transformed templates.

3. Proposed Algorithm

The proposed template security method is depicted in the Fig.1.From the public datasets, the biometric images are taken. The extracted SURF/HoG features from fingerprint, face, and signature images are to be concatenated to make it feature-level fusion. The concatenation can be carried out after reducing the feature vector dimensions (*d*) into equal size. The final versions of fused features are the original templates and have to be secured by transforming into new feature space. This work takes two template protection approaches to check its performances on multi-modal biometric recognition. One is bio-hash template protection [Teoh*et.al* (2004)]; another is non-invertible hashing protection technique [Mainguet JF. (2009)]. The protected templates are classified with the help of neural network classifier. This proposed work's steps are explained in the following sections.

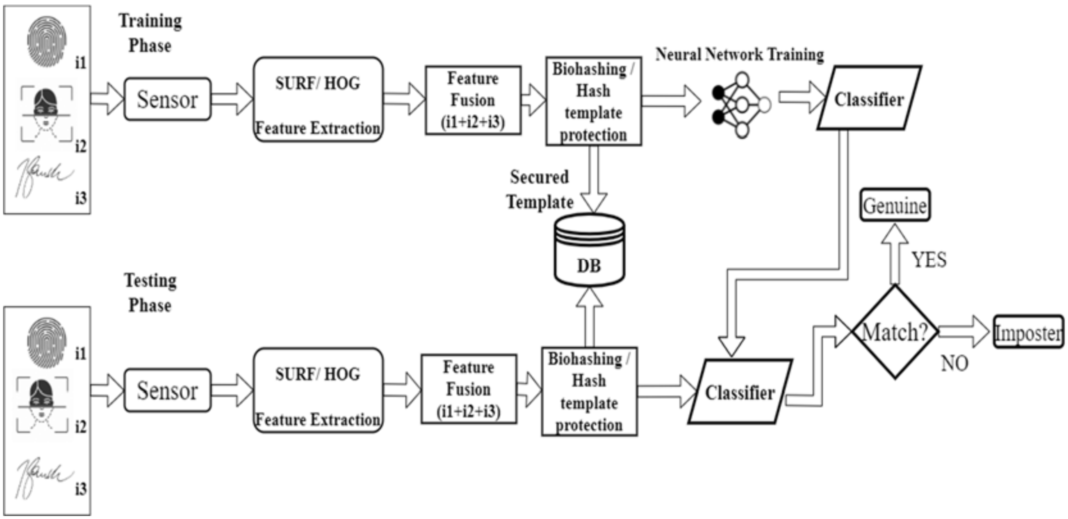


Fig1: Proposed Template security Method

3.1Feature Extraction

3.1.1 SURF

Speeded up Robust Features detection technique is considered to be a fast detector [Herbert Bay *et.al* (2008)]. The SURF technique's significant objective is based on two points. One is to detect interest points known as detectors and another is to find distinctive descriptors. The advantage of this SURF method is, the feature matching will be continued effectively even in the change of viewing conditions or in the change of geometric deformations. The detectors are extracted from an image are the distinctive interest points into a series of numerical vectors. Whereas the feature descriptors are the pixel coordinates of important areas of the input image. This SURF detector-descriptor method follows the Hessian matrix approximation technique for detecting interest points due to its good computation. These both techniques use integral images for fast calculation. An integral image$I_{\Sigma}(X)$ at a position *(X=i,j),* which is a sum of upper pixels and the pixels left to the *(i,j)* point. The integral image $I_{\Sigma}(X)$ is calculated asin "E.q.(1)".

$$I_{\sum}(X) = \sum_{i=0}^{i<x}\sum_{j=0}^{j<y} I(i,j) \qquad (1)$$

Here (i,j) is the pixel positions of image I. For every pixel of the integral image, the determinant value is calculated with Hessian matrix $H(x,\sigma)$calculated as in "Eq.(2)":

$$H(x,\sigma) = \begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \qquad (2)$$

Here $L_{xx}(x,\sigma)$, $L_{xy}(x,\sigma)$ and $L_{yy}(x,\sigma)$are the Gaussian derivatives convolution $\frac{\partial^2}{\partial_{x^2}}\, g(\sigma)$of the image I. σ is the representation of scale of the input image. But the descriptor uses Haar-wavelet responses from the interest point neighborhood. SURF descriptor is detected based on the orientation information from the spherical region of the interest point by calculating Haar-wavelet responses based on the X-Y direction. The key point is detected by calculating the horizontal and vertical wavelet responses around the interest point. While keep changing the scanning area's orientation till the largest sum value is found. The obtained final orientation is the dominant direction. The Fig.2 shows the SURF features of fingerprint, face and signature images.

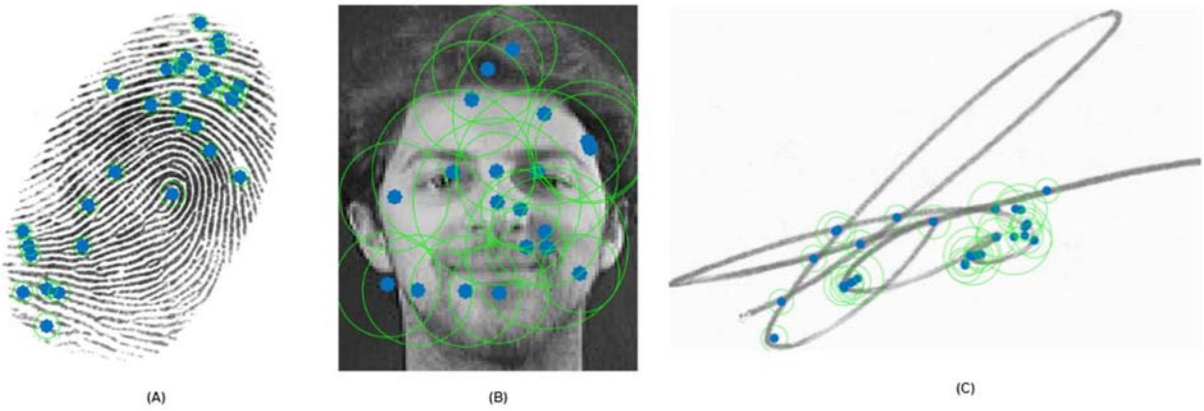


Fig 2: SURF Interest Points A) Fingerprint B) Face and C) Signature

3.1.2 Histogram of Oriented Gradients (HOG)

Histogram of Oriented Gradients is a computer vision feature extraction algorithm for detecting feature descriptors from the given image. This method is like a canny edge detector [Wang *et.al* (2009)] for object detection. HoG method's importance [NavneetDadal N*et.al* (2005)]is to find the structure of the image by counting the existences of gradient orientation on the localized portions. This descriptor discovers angle and magnitude information to calculate the feature. And also produces histograms with the angle and magnitude information. The following steps are explaining the histogram generation of the input image.

i) Input image I(x,y) is resized into 128×64 pixels for better results.

ii) The gradient of the input is computed by joining orientation (G_x) and magnitude (G_y) of the image. For every pixel $G_x$and G_y are calculated in a 3×3 block as in "E.q.(3) &E.q. (4)":

$$G_x(r,c) = I(r,c+1) - I\,(r,c-1) \qquad (3)$$

$$G_y(r,c) = I(r-1,c) - I(r+1,c) \qquad (4)$$

Here *r* is represented as row; *c* is column of the input image matrix. The overall magnitude and angle are computed as in "E.q.(5) &E.q. (6)":

$$Magnitude(\mu) = \sqrt{{G_x}^2 + {G_y}^2} \qquad (5)$$

$$Angle(\theta) = \left|\tan^{-1}\frac{G_x}{G_y}\right| \qquad (6)$$

iii) Now each pixel's gradient has been attained with non-overlapping cells by dividing 8×8 blocks. For this each 8×8 block (j), a 9-point histogram is computed. Every block has a range of 20 degree angle (θ) and 64 dissimilar values. For every value, the magnitude $\Delta\theta.j$and gradient$\Delta\theta.(j+1)$ are totaled to find jth blocks center point c_j as in "E.q.(7)":

$$c_j = \left[\frac{\Delta\theta.j + \Delta\theta.(j+1)}{2}\right] = \Delta\theta\left(j+\frac{1}{2}\right) \quad (7)$$

iv) The resulted value of jth block is v_j and the neighbor block is v_j+1. The matrices are acquired by calculating as in "E.q.(8) &E.q. (9)":

$$v_j = \mu.\left[\frac{\theta}{\Delta\theta} - \frac{1}{2}\right] \quad (8)$$

$$v_{j+1} = \left[\frac{\theta - c_j}{\Delta\theta}\right] \quad (9)$$

v) For all the blocks the above procedure is repeated for histogram computation with a stride of 8 pixels, and it produces 36 feature vectors $f_{b_i}$from 4 cells per block (b) and the 9-points of histogram are calculated. It is represented as in "E.q.(10)":

$$f_{b_i} = [b_1, b_2, b_3 \dots\dots\dots\dots..b_{36}] \quad (10)$$

The values of f_{b_i} have to be normalized by L_2 norm as in "Eq.(11)":

$$f_{b_i} = \frac{f_{b_i}}{\sqrt{\left\|{f_{b_i}}^2\right\| + \epsilon}} \quad (11)$$

The Є – is a small number to be added to avoid division error.

The size of HoG features will be (7×15×36) 3780 pixels since 36 feature vector points are gathered from 7 blocks of the horizontal direction and 15 blocks of the vertical direction from the resized input image. The following Fig.3 shows the HoG feature points of fingerprint, face and signature.

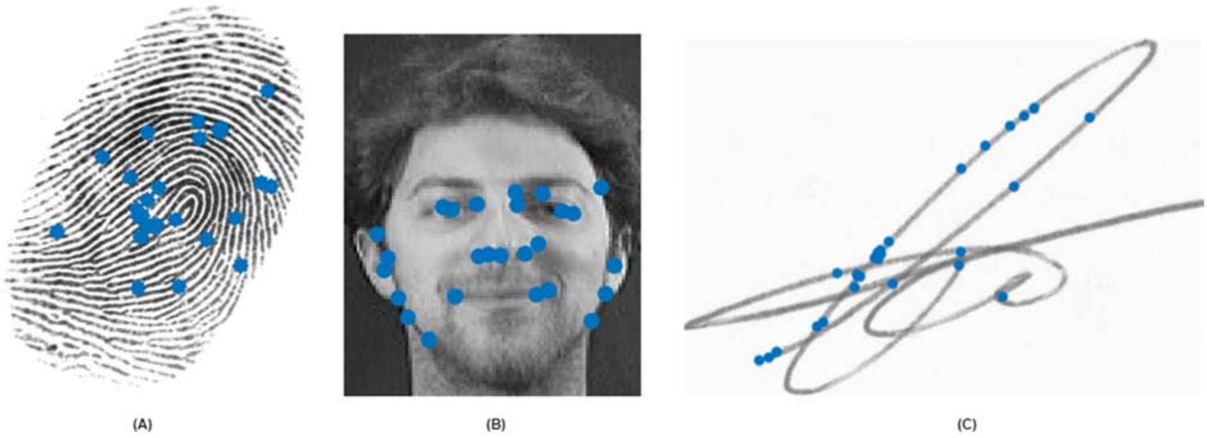


Fig 3: HoG Feature Points A) Fingerprint B) Face and C) Signature

3.2 Bio-Hash Template protection

The bio-hash technique produces a randomized matrix (*r*) equal to the fused feature vector using the seed value. The matrix *r*, $r \text{Є} R^d$, which has been uniformly distributed between [0,1]. The *r* matrix is created using a seed value (*s*), is generated by the system and the same seed value is used at the time of enrolment. This seed value is unique for every user and need not to be remembered by the user. The bio-hash template protection procedure is as follows:

i) The input images fingerprint (*F*), face(*F*), and signature(*S*), and their respective dimensions are d_x, d_y, d_z. They are represented as F^{d_x}, F^{d_y} and S^{d_z}.

ii) SURF/HoG feature extraction methods give features as numerical vectors and are represented as Ƒ$_{fv}$, Ғ$_{fv}$, S$_{fv}$. The dimensions (d_x, d_y, d_z) have to be resized in to common dimension (d), Ƒ$_{fv}$, Ғ$_{fv}$, S$_{fv}$ Є R^d.

iii) The extracted features are concatenated as C = Ƒ$_{fv}$+Ғ$_{fv}$+S$_{fv}$ЄR^d .

iv) Token (s) value is generated by the system between $[0,1]^N$ as uniformly distributed values, for N number of users.

v) Create a random pattern using the token $\{r_i$ Є $R^N\, |i=1,2,3,....N\}$.Now this random pattern has to be orthonormalized by Gram-Schmidt method. The resulted matrices are $\{r\perp_i$ Є $R^N\, |i=1,2,3,....N\}$.

vi) Calculation of inner product with the random pattern and with fused features are denoted as { <C | $r\perp_I$> Є R^N ,$i=1,2,3,....N$ }. *The* < ● | ● >signifies inner product.

vii) To make the calculated templates into binary values, compute d bits for Bio-hash (bh_iЄ 2^d) from "E.q. (12)

$$bh_i = \begin{cases} 0 \; if < \mathrm{C} \,|\, r\perp_i > \; \leq \tau \\ 1 \; if < \mathrm{C} \,|\, r\perp_i > \; \geq \tau \end{cases} \qquad (12)$$

Here τ is the threshold value and this step transforms the templates into binary values according to the threshold. Repeating this procedure, the transformed templates can be attained using the bio-hash technique.

3.3 Multiplicative Hashing

Instead of using a uni-modal biometric system, multiple modalities are needed to make a system more secure. The samples of biometric traits also increased to train the network for better classification. But usage of many samples and multiple traits takes much space than the usual system of biometric identification. To tackle this problem, this work checks the template security performance with a hashing method. Hashing is a data structure to maintain a symbol table for original information; here the fused features are transformed into hash codes. Many researchers have worked with non-invertible hashing for providing cancelability on biometric features. The authors [Lai, Yenlung*et.al*(2016] use two methods Hadamard product code and modulo thresholding function to enhance the Min-hashing method to introduce IFO (Indexing-First Order) technique. This provides IFO hashed code and survives on various attacks. Also, the non-invertible hash code is generated from vector permutation and a shift-order process to bring a non-invertible scheme for fingerprint preservation [Abdullahi, Sani *et.al* (2021)]. But the present work applies the multiplicative hash method to the fused features for transforming into non-invertible templates. The multiplicative hash method is in "E.q. (13)":

$$h(k) = \lfloor m(kA \; mod \; 1) \rfloor \qquad (13)$$

Constant A (kA) represents in the range $0<A<1$. The fractional portion is extracted from kA with $mod\ 1$ operation. Again this fractional part is multiplied with m $(m=2^p)$ and the floor of the result is taken. The p is some integer value of highest-order bits. The fused features of three modalities' feature vectors are taken as k here. The system generated seed value is taken as constant A to multiply with the features. Once created the hash codes, these are given as sequence to the LSTM neural network for classification.

3.4 Feature classification based on LSTM neural network range

A matching process is a comparison between the query's features with the database storage. It produces a matching score and it must give a decision whether the enrolled templates match with stored templates. The matching techniques are sorted [Alonso-Fernandez *et.al.*(2008)] from basic distance algorithms to sophisticated techniques like support vector machines, thresholding techniques, multistage matching, classification, indexing, etc. This work proposes a continuous classification refers with the main feature vector representation. This can be extremely fast matching and it is considered to be an error-free modal. To do this, recurrent neural network's advanced version LSTM (Long Short-Term Memory) neural network is adopted to provide numerical inputs as sequence basis. LSTM network has feedback connections and it is well-suited for predicting, processing, and classification of sequential data.

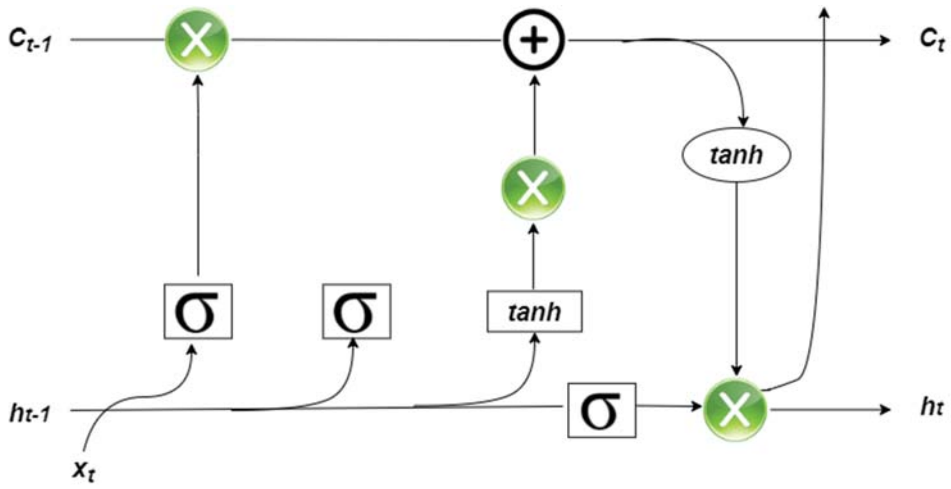


Fig 4: The Long Short-Term Memory (LSTM) method keeps its hidden state and it processes the data sequentially

The LSTM comprises a cell; a gate for input, a gate for output and a forget gate as in Fig.4. Each cell of LSTM unit remembers the incoming values on time intervals and information flow is regulated by the three gates. Variables used in the LSTM network are tabulated in table, e.g.Table.1.

Variables	**Definition**
$x_t Є R^d$	LSTM unit's input vector
$f_i Є (0,1)^h$	Activation vector of forget gate
$i_t Є (0,1)^h$	Activation vector of input gate
$O_t Є (0,1)^h$	Activation vector of output gate
$h_t Є (-1,1)^h$	Hidden state vector
$C_t Є R^h$	Vector of cell state
$\tilde{C}_t \in R^h$	Activation vector of input cell

Table 1: The LSTM Network's Variables

W_tЄ $R^{h\times d}$, U_tЄ $R^{h\times}$, b Є R^h: *W* and *U* are weight matrices and the *b* is a parameter for bias vector. *d* and *h* are the input features count and the count of hidden units respectively. The sigmoid activation function is σ_g, the tangent (tanh) activation function is σ_c. Forget gate of LSTM unit has some equations as in "E.q.(13), E.q.(14), E.q.(15), E.q.(16), E.q.(17) and E.q.(18)" to be given as forwarding manner.

$$f_i = \sigma_g\left(W_f x_t + U_f h_{t-1} + b_f\right) \qquad (14)$$

$$i_t = \sigma_g(W_i x_t + U_i h_{t-1} + b_i) \qquad (15)$$

$$O_i = \sigma_g(W_o x_t + U_o h_{t-1} + b_o) \qquad (16)$$

$$\tilde{C}_t = \sigma_c(W_c x_t + U_c h_{t-1} + b_c) \qquad (17)$$

$$C_t = f_t{}^\circ C_{t-1} + i_t{}^\circ \tilde{C}_t \qquad (18)$$

$$h_t = O_t{}^\circ \sigma_{t-1}(C_t) \qquad (19)$$

Initially $C_o = 0$ and h_o=0, ° denotes element-wise product and *t* denotes time step. The LSTM cell state transfers significant information in the sequence chain known as the network's "memory". Even in the later time steps, the gates can learn information that is relevant during the training process. In the proposed work the protected templates are given to this LSTM network as sequence basis. This will predict the input query with the supervised learning of trained protected templates.

4 Results and Discussions

The proposed method has been experimented to find the performances based on the two different techniques under SURF and HOG feature extraction algorithms. One is no-protection method that calculates the parameters such as, AUC (Area under Curve), EER (Equal Error Rate), Accuracy, Specificity, Sensitivity, FAR(False Acceptance Rate), F1-score, FNR (False Negative Rate) before using the protection techniques. The other method is to calculate the same parameters after providing template protection. To make the differences in feature extraction step, the proposed system chooses four ways. Extract 10 strongest SURF/HOG points from multiple modalities, and giving protection using one of the methods discussed here and trains the system with LSTM network for making prediction. The same process is carried out by extracting 20, 30, 40 strongest points to find if any changes are happening when the feature point count has been changed. Table 2, Table 3, and Table 4 show the performance matrices over the different feature extraction methods on no-protection method, bio-hashing protection technique, and hash method with different counts of feature extraction points. The accuracy is calculated from True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) as in “E.q. (20), E.q.(21), E.q.(22), E.q.(23), E.q.(24) and E.q.(25) .

$$accuracy = \frac{TP+TN}{TP+FP+FN+TN} \tag{20}$$

$$specificity = \frac{TN}{TN+FP} \tag{21}$$

$$sensitivity = \frac{TP}{TP+FN} \tag{22}$$

$$FAR = \frac{FP}{FP+TN} \tag{23}$$

$$FNR = \frac{FN}{FN+TP} \tag{24}$$

$$f1\ score = 2 \times \frac{GAR \times sensitivity}{GAR+sensitivity} \tag{25}$$

GAR is the genuine acceptance rate which is calculated as TP/ (FP+FP). AUC is a curve to represent the probability measurement to identify the performance at different thresholds. It shows the capability of the model that how much it is efficient in differentiating between classes. If the AUC is high, the model is good in predicting the 1 classes as 1 and 0 classes as 0. The proposed model’s classification probability has been plotted here to show the performance measures on three diverse methods at different thresholds in the below figures.

No-protection Method	**SURF**				**HOG**			
	10 Points	**20 Points**	**30 Points**	**40 Points**	**10 Points**	**20 Points**	**30 Points**	**40 Points**
AUC	0.06	0.61	0.26	0.65	0.34	0.34	0.32	0.5
EER	0.94	0.39	0.74	0.35	0.66	0.66	0.68	0.5
Accuracy	0.66	0.38	0.67	0.66	0.71	0.73	0.72	0.48
Specificity	0.66	0.53	0.66	0.66	0.69	0.72	0.71	0.59
FAR	0.33	0.46	0.33	0.33	0.3	0.27	0.28	0.4
Sensitivity	1	0.01	1	1	1	0.92	0.82	0
F1-score	0.019	0.01	0.05	0.01	0.23	0.37	0.37	DIV/0
FNR/FRR	0	0.98	0	0	0	0.08	0.17	1

Table 2: Performance matrices if no-protection is given on Multi-modal biometric system

Bio-hashing Method	**SURF**				**HOG**			
	10 Points	**20 Points**	**30 Points**	**40 Points**	**10 Points**	**20 Points**	**30 Points**	**40 Points**
AUC	0.1	0.36	0.42	0.18	0.55	0.47	0.03	0.34
EER	0.9	0.64	0.58	0.82	0.45	0.53	0.97	0.66
Accuracy	0.57	0.67	0.66	0.66	0.64	0.59	0.65	0.67
Specificity	0.63	0.67	0.66	0.66	0.66	0.64	0.66	0.66
FAR	0.36	0.32	0.33	0.33	0.33	0.35	0.33	0.33
Sensitivity	0.03	1	1	1	0.39	0.11	0.36	1
F1-score	0.01	0.05	0.01	0.019	0.14	0.04	0.07	0.03
FNR/FRR	0.96	0	0	0	0.6	0.88	0.63	0

Table 3: Performance matrices if Bio-hash protection is given on Multi-modal biometric system

Hashing Method	**SURF**				**HOG**			
	10 Points	**20 Points**	**30 Points**	**40 Points**	**10 Points**	**20 Points**	**30 Points**	**40 Points**
AUC	0.5	0.5	0.57	0.6	0.66	0.5	0.44	0.48
EER	0.5	0.48	0.43	0.4	0.34	0.5	0.56	0.52
Accuracy	0.99	0.99	0.99	0.99	0.8	0.76	0.78	0.78
Specificity	0.99	0.99	0.99	0.99	0.77	0.74	0.75	0.76
FAR	0.005	0.005	0.005	0.005	0.22	0.25	0.24	0.23
Sensitivity	1	1	1	1	1	0.97	0.97	0.97
F1-score	0.99	0.99	0.99	0.99	0.6	0.48	0.53	0.54
FNR/FRR	0	0	0	0	0	0.02	0.02	0.02

Table 4: Performance matrices if hashing protection is given on Multi-modal biometric system

The following plots show the TPR (True positive rate) on the y-axis against FPR (False positive rate) on the x-axis. Fig.5a is the plot of SURF's strongest 10 points extraction and Fig.5b is the plot of HOG's strongest 10 points. It displays that the hashing protection method's AUC curve is higher than the other two methods of bio-hash and no-protection.

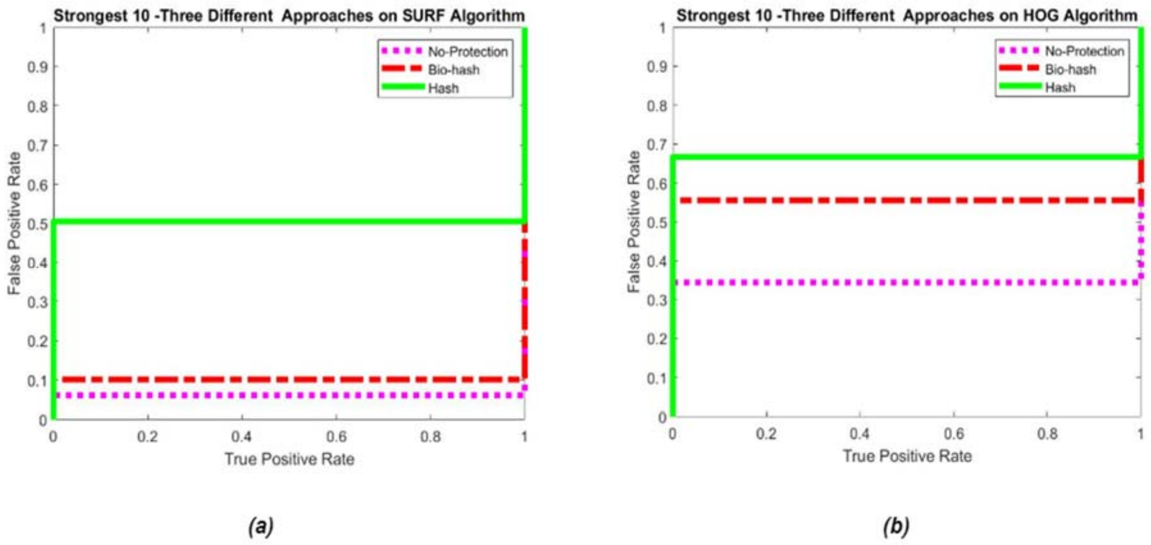


Fig 5: Strongest 10 interest points tested with three different methods on a) HOG b) SURF

After extracting strongest 20 points using HOG, the proposed method is applied and plotted in Fig 6a. In this, the hash protection has a higher AUC other than the two techniques. But while extracting 20 SURF points, it gives higher AUC at no-protection method as showed in Fig 6b. If the strongest 30 interest points are extracted using HOG and SURF, the proposed hash method gives higher AUC on both as depicted in Fig7a. and 7b. When the strongest 40 points are extracted using both algorithms, the higher performance is on no-protection method as shown in Fig 8a and Fig 8b. The strongest 10, 20, and 30 points give higher AUC on hashing template protection. If 10 more interest points are extended after 30, both template secure method's AUC goes lower than the no-protection procedure. According to the need of the recognition system, the extracted points maybe till 30 unique features. When compared to the no-protection method and bio-hash secure method, the hashing template security gives good performances on multi-modal biometric recognition.

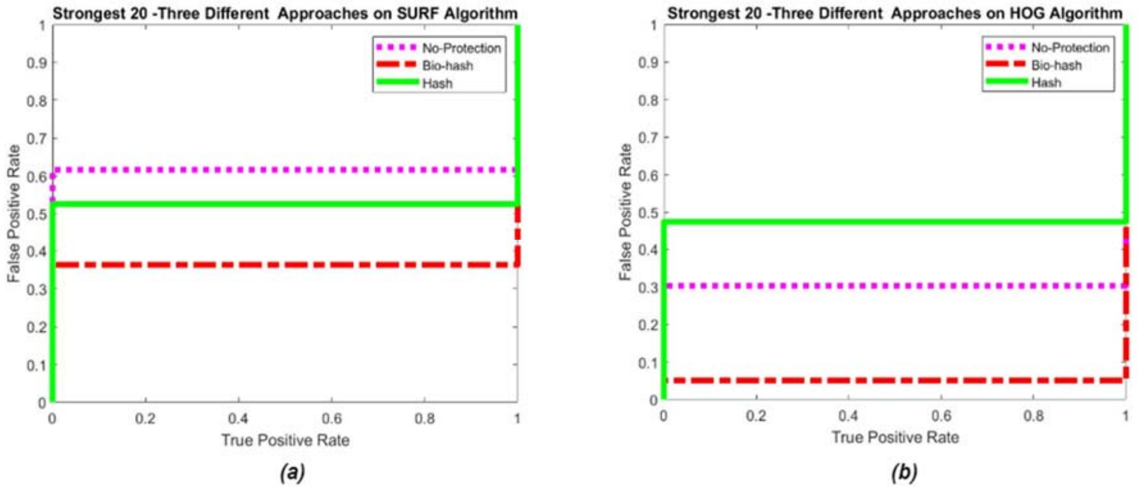


Fig 6: Strongest 20 interest points tested with three different methods on a) HOG b) SURF

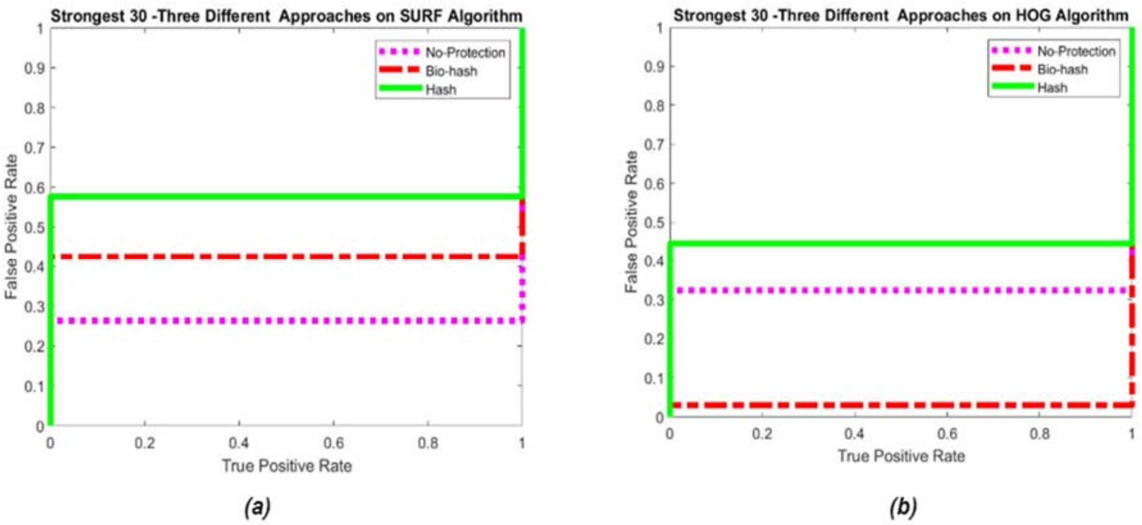


Fig 7: Strongest 30 interest points tested with three different methods on a) HOG b) SURF

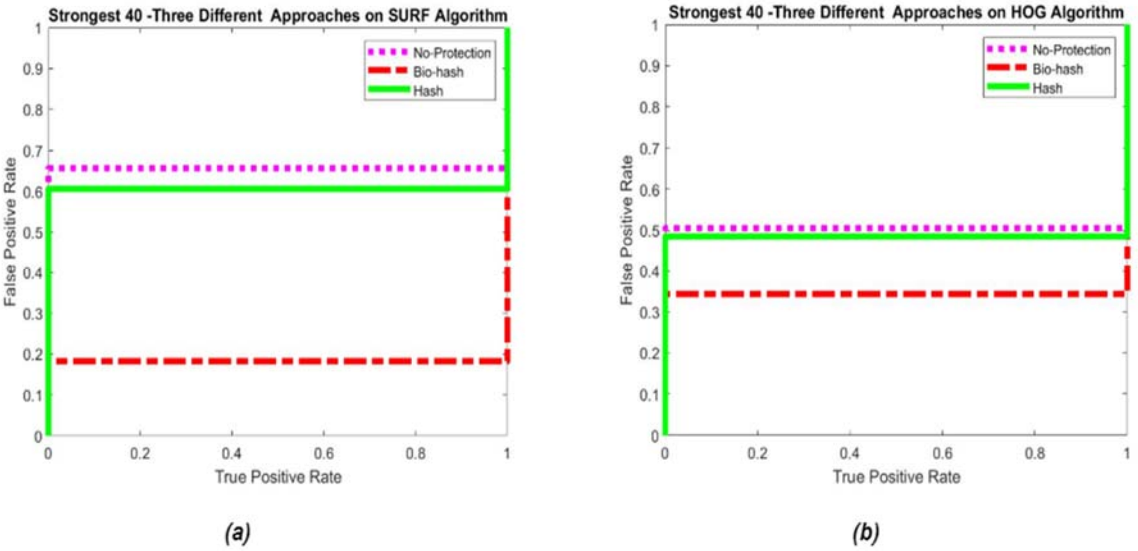
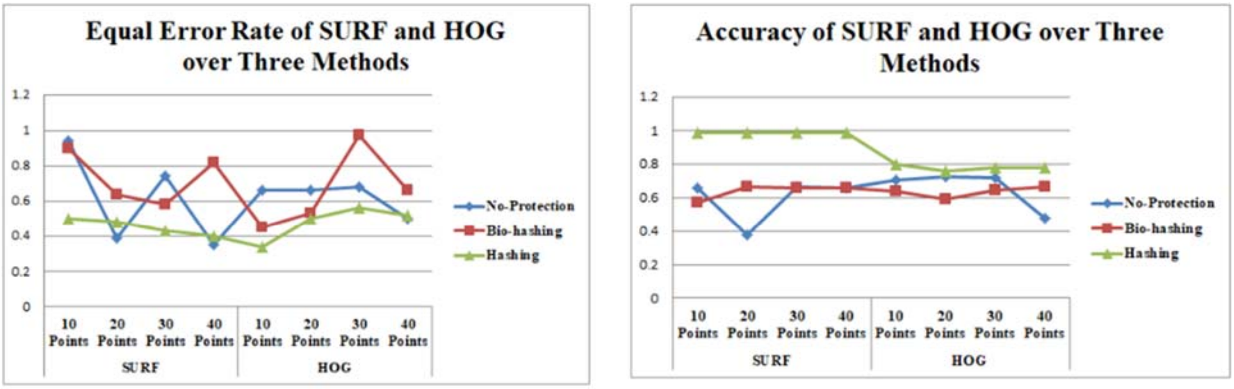


Fig 8: Strongest 40 interest points tested with three different methods on a) HOG b) SURF

The EER is another performance measure of the proposed system under TPR and FPR. Usually the EER is calculated when the true positive rate and false positive rate meets at the same point. Lower the EER value is the good sign of system performance. The proposed system also computed the EER against the three techniques. The chart as in Fig 9a. depicts the EER performance of no-protection, bio-hashing and hashing methods. It clearly says that hashing template preservation technique gives lower EER value than the other two on all the different counts of strongest points and with both feature extraction method. The accuracy of the methods is also depicted as chart in Fig 9b. and it states that hashing give highest accuracy rate on all the four interest point counts and also on the two different feature extraction method. Whatever may be the interest point counts and the interest point extraction algorithms, the hashing protection shows good performance over others. The lowest EER found at strongest 10 points extracted using HOG over hashing technique. All the SURF’s strongest four counts give highest accuracy than HOG at hashing protection.



(a) (b)

Fig 9: a) EER and b) Accuracy of HOG and SURF Algorithms on no-protection, Bio-hash protection and Hash protection

5 Conclusion

Revocable multi-modal biometric template privacy-preservation based on bio-hash and simple hash methods have been proposed in this work. Fingerprint, face, and signature are fused at the feature-level after extracting features using computer vision algorithms of SURF and HoG. Both methods need a seed value that has been generated by the system instead of user-specific data. According to the specific value, the random matrix is generated for every user to transform the features into a new feature space. The experimental results depict that the highest accuracy is reached at the simple hashing method than bio-hash and unprotected. The advantage of this work is that the user does not need to remember the key due to the system creation of seed value at the time of enrollment and it will be maintained. This proposed investigation calculated accuracy, EER, sensitivity, specificity, FAR, f-score to find the performance of the proposed method. The highest accuracy is achieved as 99% and the lowest EER value has been obtained as 0.34 if simple hashing template preservation is applied. When compared with bio-hash protection, simple hash template protection outperforms in terms of different performance metrics as well as at various feature counts.

In future, this work will be extended with hybrid feature extraction and hybrid template preservation. The time taken by classification network and time taken by conventional matching technique will be calculated in the extended work.

References

[1] Jain A.K., Ross A. (2008) *Introduction to Biometrics*. In: Jain A.K., Flynn P., Ross A.A. (eds) Handbook of Biometrics. Springer, Boston, MA.

[2] Clifton L. Smith., David J. Brooks (2013) Chapter 7- Integrated Identification Technology, In: Clifton L. Smith., David J. Brooks (eds) Security Science, Butterworth-Heinemann. Pp.153-174

[3] Zhao, W., &Chellappa, R. (2006): Face processing: advanced modeling and methods. Amsterdam: Elsevier / Academic Press.

[4] Kumar, Munish&Dargan, Shaveta. (2019): A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities. Expert Systems with Applications. Pp. 1-27.

[5] Toli, Christina-Angeliki&Preneel, Bart. (2014): Multimodal Biometrics and the Protection of their Templates. IFIP Advances in Information and Communication Technology. 457.

[6] Y. H. Dandawate and S. R. Inamdar, (2015): Fusion based Multimodal Biometric cryptosystem, 2015 International Conference on Industrial Instrumentation and Control (ICIC), pp. 1484-1489.

[7] Teoh, Andrew &Kuan, Yip & Lee, Sangyoun. (2008): Cancelable biometrics and annotations on BioHash. Pattern Recognition. 41. 2034-2044. 10.1016/j.patcog.2007.12.002.

[8] D. Ahn, S. G. Kong, Y. Chung and K. Y. Moon, (2008): Matching with Secure Fingerprint Templates Using Non-invertible Transform, 2008 Congress on Image and Signal Processing, 2008, pp. 29-33.

[9] I. Raghu and V. Sreelatha Reddy, (2014): Key binding with fingerprint feature vector, 2014 International Conference on Computer Communication and Informatics, pp. 1-5.

[10] N. Lalithamani and K. P. Soman, (2009): An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancelable Fingerprint Biometrics, 2009 International Conference on Advances in Recent Technologies in Communication and Computing, pp. 47-52.

[11] K, Krishna Prasad and Aithal, P. S., (2017): A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User (December 28, 2017). International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126.

[12] You L., Li X. (2018): A Cancelable Multi-Biometric Template Generation Algorithm Based on Bloom Filter. In: Vaidya J., Li J. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2018. Lecture Notes in Computer Science, 11336. Springer, Cham.

[13] Paul, Padma Polash&Gavrilova, Marina. (2015): Feature and Rank Level Fusion for Privacy Preserved Multi-Biometric System. International Journal of Software Science and Computational Intelligence. 7. Pp. 1-17.

[14] Gupta, K., Walia, G.S. & Sharma, K. (2021): Novel approach for multimodal feature fusion to generate cancelable biometric. Vis Comput 37, pp.1401–1413.

[15] H. Kaur and P. Khanna, (2019): Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features," in IEEE Transactions on Information Forensics and Security,14(3), pp. 709-719.

[16] Abdellatef, E., Ismail, N.A., AbdElrahman, (2020): S.E.S.E. et al. Cancelable multi-biometric recognition system based on deep learning. Vis Comput 36, pp.1097–1109.

[17] R. Belguechi, E. Cherrier and C. Rosenberger, (2012): Texture based fingerprint BioHashing: Attacks and robustness," 2012 5th IAPR International Conference on Biometrics (ICB), pp. 196-201.

[18] Fatima, Bedad&Adjoudj, Reda. (2018). Secured Multimodal Biometric System. Journal of Multimedia Processing and Technologies. 9. 77.

[19] Aithal, Sreeramana&Karani, Krishna Prasad. (2017): A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS). 2. Pp.116-126.

[20] Tulyakov, Sergey &Farooq, Faisal &Govindaraju, Venu. (2005): Symmetric Hash Functions for Fingerprint Minutiae. Int Workshop on Pattern Recognition for Crime Prevention (LNCS: 3687), Security and Surveillance. Pp.30-38.

[21] V. Talreja, S. Soleymani, M. C. Valenti and N. M. Nasrabadi, (2019): Learning to Authenticate with Deep Multibiometric Hashing and Neural Network Decoding, ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. pp.1-7,

[22] Ashok A., Poornachandran P., Achuthan K. (2012): Secure Authentication in Multimodal Biometric Systems Using Cryptographic Hash Functions. In: Thampi S.M., Zomaya A.Y., Strufe T., AlcarazCalero J.M., Thomas T. (eds) Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2012. Communications in Computer and Information Science, vol 335. Springer, Berlin, Heidelberg.

[23] Z. Jin, J. Y. Hwang, Y. Lai, S. Kim and A. B. J. Teoh, (2018): Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing, in IEEE Transactions on Information Forensics and Security, 13(2), pp. 393-407.

[24] Teoh, Andrew & Ngo, David &Goh, Alwyn. (2004): Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition. 37. Pp.2245-2255.

[25] Mainguet JF. (2009): Fingerprints Hashing. In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_60

[26] Herbert Bay, Andreas Ess, TinneTuytelaars, and Luc Van Gool. (2008): Speeded-Up Robust Features (SURF). Comput. Vis. Image Underst. 110, 3 (June, 2008), pp.346–359.

[27] Wang, B., & Fan, S. (2009): An Improved CANNY Edge Detection Algorithm. 2009 Second International Workshop on Computer Science and Engineering, 1,pp. 497-500.

[28] NavneetDadal N. Dalal and B. Triggs, (2005): Histograms of oriented gradients for human detection, 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 2005, pp. 886-893 vol. 1.

[29] Lai, Yenlung& Jin, Zhe&Goi, Bok-Min & Chai, Tong-Yuen & Yap, Wun-She. (2016): Iris Cancellable Template Generation Based on Indexing-First-One Hashing. 9955. 450-463. 10.1007/978-3-319-46298-1_29.

[30] Abdullahi, Sani&Shuifa, Sun. (2021): Random Hash Code Generation for Cancelable Fingerprint Templates using Vector Permutation and Shift-order Process.

[31] Alonso-Fernandez, Fernando &Fierrez, Julian. (2008): Encyclopedia of Biometrics.

Authors Profile

B.Nithya, is a Ph.D.Research scholar of VISTAS, Chennai. She has completed M.Phil in computer science at VISTAS, Chennai, Tamil nadu in 2017. Her research interests are biometric templates security, security of information transferred through communication medium. She has published 3 research articles under SCOPUS. Also she is interested in programming languages such as Java, C#, python and frameworks like MATLAB and .net programming. Her area of interest is image processing.

Dr.P.Sripriya, presently she is working as a professor in Computer Application department at VISTAS, Chennai, Tamil Nadu. Her educational qualification is M.C.A, M.Phil, Ph.D. She has 22 years of working experience in teaching profession. She has published 22 research articles under SCOPUS. Her areas of interests are Image Processing, Big Data and Data Mining.