ISSN 1533-9211

DOI 10.17605/OSF.IO/2RTXH

A NOVEL APPROACH FOR HAND BASED CANCELABLE BIOMETRIC AUTHENTICATION SYSTEM USING K-FOLD CROSS VALIDATION SCHEME

ANUP RITTI[1], Dr. V. N. RAJAVARMAN[2] and Dr.D.USHA[3]

[1] Research Scholar, Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai, India. Email: anup.ritti66@gmail.com
[2] Professor, Computer Science and Engineering, Dr M.G.R Educational and Research Institute, Chennai, India. Email: nrajavarman2003@gmail.com
[3] Professor, Computer Science and Engineering, Dr M.G.R Educational and Research Institute, Chennai, India. Email: usha.cse@drmgrdu.ac.in

Abstract

Biometrics are in the trend as it reduces risk and quite difficult to replicates. Currently most popular biometrics such as fingerprint, retina can be forged. Dorsal Vein pattern is gaining attention these days due to its contactless nature and difficult to forge. These vein patterns can give rise to another reliable biometric which better than the biometrics being currently used. Various cancellable biometric techniques have been proposed to maintain user data security. A cancellable biometric framework is introduced to satisfy user data security and keeping the original biometric template safe away from intruders. Biometrics like fingerprints and retinas are very vulnerable at the moment. Contactless, and thus impossible to counterfeit, has made the dorsal vein pattern a hot topic these days. This pattern can provide another more reliable biometric that is already in use. Currently, both the academic community as well as sector are paying attention to the results of hand vein patterns towards biometric authentication. In this paper, our proposed K-fold cross validation technique based on cancelable biometrics has been tested and it is delivering the good result as compared to the techniques such as SURF and BRISK algorithms which shows less accuracy.

Index Terms: Cancellable biometric, Dorsal hand vein, K-fold Cross validation, BRISK and SURF

1. INTRODUCTION

A biometric system uses signature points of measurable uniqueness, derived from the physiological and/or behavioural characteristics possessed by an individual, to characterize and determine his/her identity. Biometric characteristics are preferably used in security systems over more traditional security measures. They are also used in internet access, computer system security, secure electronic passport control, banking, mobile phones, credit cards, secured access to buildings, health and social services, parenthood determination, terrorist determination and corpse identification. A number of relevant biometric technologies have been developed based on diverse biometric cues, such as DNA [1], ear morphology [2], facial features [3], fingerprints [4], gait [5], hand and finger geometry [6], iris [7], keystroke [8], odor [9], palm print [10], hand writing and signature [11], voice [12], etc.

Biometrics is an excellent system for security used in various platforms such as industry, banking, and mobile phones. Presently, many methods are available to verify individual identities, such as fingerprint recognition, voice recognition, retinal scans, and facial recognition.

These systems also pose a risk of compromising biometric information in many ways, such as fingerprints can be hacked from glass panels or other locations by mimicking their fingerprints. In the past, fingerprint systems have repeatedly been hacked by the sticky fingerprint method.

To address this problem and to provide better preservation of information, we are attempting to develop a biometric detection system based on the idea of cancellable biometric.

1.1 Biometric Authentication System

Biometric authentication is a process in which a person's identity is verified based on specific biological characteristics. In biometric authentication, first, a person's biometric information is captured and then matched with the data stored in the database. If both data (captured and stored) match, the authentication is confirmed.

Biometric authentication is the most effective and secures authentication system because a person's biological information is unique. It is possible that a person's password and unique ID can be stolen and misused. Biometric identity is always safe, cannot be leaked, and very difficult to transfer from one person to another.

1.2 Cancellable Biometric Authentication

Since biometric authentication is a widely used authentication system in various departments and is stored digitally in a database, there are chances that someone can steal a piece of biometric information by invading the database and misuse its confidential information.

To avoid such attacks and secure our data, we can use the cancellable biometric authentication system. To protect biometric information in this cancellable biometric system, we intentionally and repeatedly distort the user's biological data.

Templates are responsible for the distortion in the feature by which the original data transformed into some other information. When an attacker tries to steal data, he gets changed information instead of the original information. To secure the user's information and deactivate the stolen data is done by changing the template information, which changes all previous biometric information in the database.

1.3 Dorsal Hand Vein Pattern

Vein pattern is the network of blood vessels beneath person’s skin. The idea using vein patterns as a form of biometric technology was first proposed in 1992. According to Li Xueyan and Guo Shuxu Vein patterns are sufficiently different across individuals, and they are stable unaffected by ageing and no significant changed in adults by observing. It is believed that the patterns of blood vein are unique to every individual, even among twins.

Contrasting with other biometric traits, such as face or fingerprint, vein patterns provide a really specific that they are hidden inside of human body distinguishing them from other forms, which are captured externally. Veins are internal, thus this characteristic makes the systems highly secure, and they are not been affected by the situation of the outer skin (e.g. dirty hand).

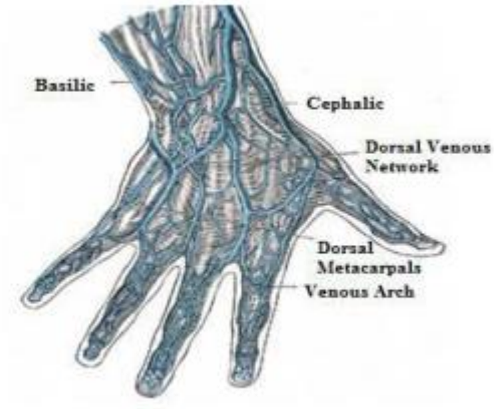


Fig 1: Drawing of the vascular network in the hand

At the same time, vein patterns can be acquired by infrared devices by two ways, noncontact type and contact type. In the case of non-contact method, there is no need to touch the device, and therefore it is friendly to individuals in the target population who utilize the systems. In the contact type, the collection type is the same as fingerprint which has already been accepted by most people.

The fig 1 illustrates the generic vascular map found on the dorsum of the hand. There are mainly two types of hand veins found on the dorsum of the hand, namely cephalic and basilic. The basilic veins are the group of veins attached with surface of hand. It generally consists of upper limb of the back of hand. Cephalic veins are the group of veins attached with the elbow of the hand.

2. LITERATURE REVIEW

Bansal and Garg et al., [13] presents a cancellable biometric template protection scheme based on the format-preserving encryption and Bloom filters. The format-preserving encryption encrypts the biometric template, which then maps to the Bloom filter based template that represents the cancellable template. The use of format-preserving encryption along with Bloom filters helps to achieve the security of the input biometric template and identification with good recognition performance. We achieve 0.2% FRR at 0.01% FAR for IITD-CASIA virtual dataset in the uni-biometric scenario.

Yang et al., [14] proposed a feature-adaptive random projection based method, in which the projection matrixes, the key to the ARM, are generated from one basic matrix in conjunction with local feature slots. The generated projection matrixes are discarded after use, thus making it difficult for the adversary to launch the ARM. Moreover, the random projection in the proposed method is performed on a local-feature basis. This feature-adaptive random projection can mitigate the negative impact of biometric uncertainty on recognition accuracy, as it limits the error to part of the transformed feature vector rather than the entire vector. The proposed method is evaluated on four public available databases FVC2002 DB1-DB3 and FVC2004 DB2. The experimental results and security analysis show the validity of the method.

ISSN 1533-9211

DOI 10.17605/OSF.IO/2RTXH

Pititheeraphab Y et al., [15] presents the development of a hybrid feature—dorsal hand vein and dorsal geometry—modality for human recognition. The proposed hybrid feature extraction method exploits two types of features: dorsal hand geometric-related and local vein pattern. In this study, the algorithm was tested on a database of 140 subjects, in which ten different dorsal hand geometric-related images were taken for each individual, and yielded the promising results. In this regard, we have achieved an equal error rate (EER) of 0.243%, indicating that our method is feasible and effective for dorsal vein recognition with high accuracy. This hierarchical scheme significantly improves the performance of personal verification and/or identification.

In Chang et al., [16] the bit-wise encryption scheme and fuzzy extractor are combined to generate a cancellable template. High security is provided on the assumption that obtaining access to one biometric template by an attacker is equivalent to getting both biometric templates of the user.

Inshirah Rossan et al. [17] has used different pre-processing techniques that causes well defined extracted vein pattern that gives better performance and leads to a more secure biometric authentication system.

R. Raghavendra et al. [18] have used a DMK 22BUC03 monochrome CMOS camera with a resolution of 744 × 480 pixel for image capture. The camera is equipped with a T3Z0312CS lens with a focal length of 8mm. To obtain the vein pattern, a region of interest (ROI) was defined using eight different feature extraction schemes that schemes include both local and global feature representation.

Yiding wang et al., [19] have explored the vein pre-processing phase. In this work the vein pattern was segmented based on simple Thresholding using gray-level distribution.

3. PROPOSED WORK

The proposed research work is given below:

3.1 Cancellability

Biometric systems have been repeatedly hacked using technique like database attack. Therefore, we are trying to develop a biometric identification system based on the idea of "Cancellable Biometrics" using a template protection approach generating binary features which are revocable.

To protect our digital biometric information, we convert it to non-invertible transformed information and attacker unable to get original information because transformed data is non-invertible. As we saw in literature review that there are many available methods to provide protection on data like bio hashing, random slop, and X-OR methods.

Implemented Cancellability functionality in our biometric system is shown below in Fig 2:

DOI 10.17605/OSF.IO/2RTXH

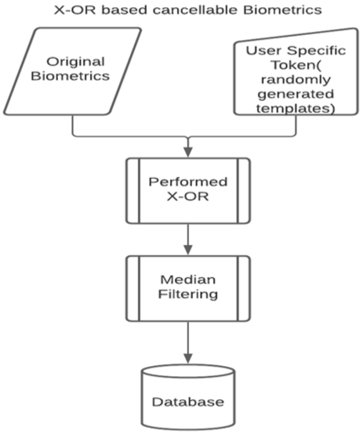

X-OR based cancellable Biometrics
Original Biometrics
User Specific Token(randomly generated templates)
Performed X-OR
Median Filtering
Database

Fig 2: X-OR based Cancellable Biometrics

3.2 K-fold Cross Validation

Cross-validation is a resampling procedure used to evaluate machine learning models on a limited data sample.

The procedure has a single parameter called k that refers to the number of groups that a given data sample is to be split into. As such, the procedure is often called k-fold cross-validation. When a specific value for k is chosen, it may be used in place of k in the reference to the model, such as k=10 becoming 10-fold cross-validation.

In k-fold cross-validation, all the samples of a person are randomly partitioned into k equal sized subgroups. Of the k subgroups, a single subgroup is taken as the validation data group for testing the model and the remaining subgroups are used as training data. This process is then repeated k times (the folds), with each of the k subgroup used exactly once as the validation data. Results obtained over k-iterations are averaged produce a single estimation. One of the advantages of this method is that all observations are used for both training and validation. In our project, we have used k-fold cross validation for k=1.

First, we need to define k that represents a number of folds. Usually, it’s in the range of 3 to 10, but we can choose any positive integer. After that, we split the data into k equal folds (parts). The algorithm has k-1 steps where at each step, we select different folds for the test set and the remaining folds we leave for the training set.

Using this method, we will train our model k-1 times independently and have k-1 scores measured by some of the selected metrics. Lastly, we can average all scores or even analyze their deviations. We presented the whole process in the Fig 3 below:

The Seybold REPORT

ISSN 1533-9211

DOI 10.17605/OSF.IO/2RTXH

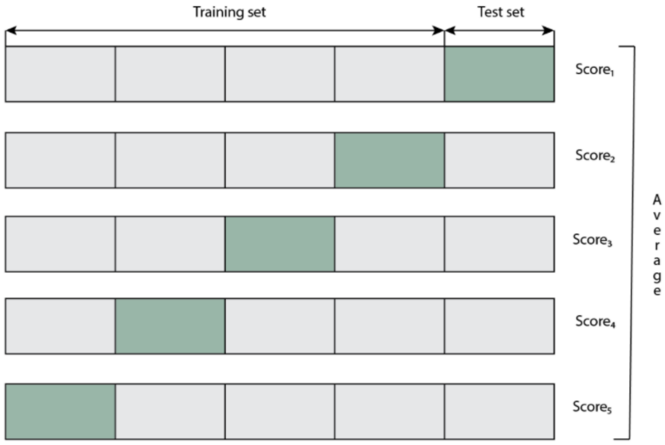
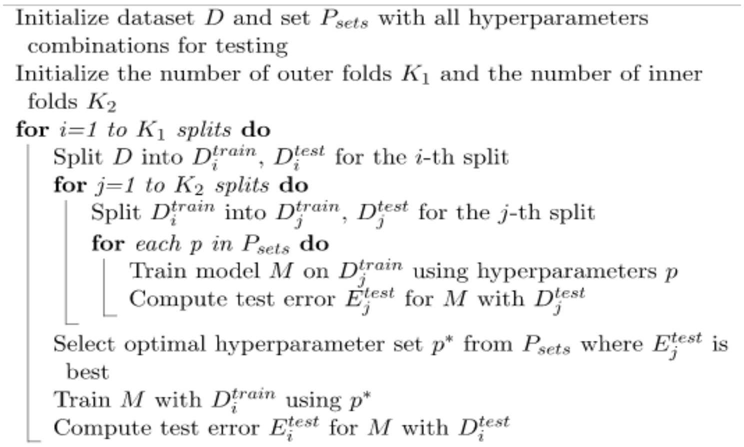


Fig 3: K-fold cross validation Scheme

K-Fold Cross validation Algorithm is given below:



```
Initialize dataset $D$ and set $P_{sets}$ with all hyperparameters
  combinations for testing
Initialize the number of outer folds $K_1$ and the number of inner
  folds $K_2$
for $i$=1 to $K_1$ splits do
    Split $D$ into $D_i^{train}$, $D_i^{test}$ for the $i$-th split
    for $j$=1 to $K_2$ splits do
        Split $D_i^{train}$ into $D_j^{train}$, $D_j^{test}$ for the $j$-th split
        for each $p$ in $P_{sets}$ do
            Train model $M$ on $D_j^{train}$ using hyperparameters $p$
            Compute test error $E_j^{test}$ for $M$ with $D_j^{test}$
    Select optimal hyperparameter set $p^*$ from $P_{sets}$ where $E_j^{test}$ is
      best
    Train $M$ with $D_i^{train}$ using $p^*$
    Compute test error $E_i^{test}$ for $M$ with $D_i^{test}$
```

3.2.1 K-fold Cross Validation with different random keys

K-fold cross validation is performed by changing the randomly generated key (as defined in the section “Non-invertible transformations”) for transformation purpose. Results have been generated for 5 different keys.

3.3 SURF and BRISK algorithms

SURF (Speeded-Up Robust Features) alogorithm is a local descriptor and works using local gradient computaions. The SURF method is a fast and robust algorithm for local, similarity invariant representation and comparison of images. The main interest of the SURF approach lies in its fast computation of operators using box filters, thus enabling real-time applications such as tracking and object recognition [20].

BRISK (Binary Robust InvariantScalable Keypoints) algorithm is a binary descriptor that relies on pairs of local intensity differences. BRISK description is based on identifying the characteristic direction of each feature for achieving rotation invariance. To cater illumination invariance results of simple brightness tests are also concatenated and the descriptor is constructed as a binary string. BRISK features are invariant to scale, rotation, and limited affine changes [21].

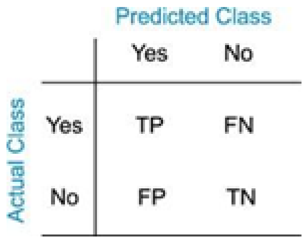
3.4 Evaluation of Performance Parameters

Performance parameters have been calculated using various methods like –

3.4.1 Confusion Matrix for Multi-Class Classification System

A confusion matrix is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known. For multi-class model one of the class is assumed as positive and other as negative and then confusion matrix is calculated. Same exercise is repeated for all the classes. Confusion Matrix consists of following values –

- True Positives (TP): These are cases in which we predicted positive and actual class is positive as well.
- True Negatives (TN): We predicted negative and actual class is negative as well.
- False Positives (FP): We predicted positive, but actually it is negative (Also known as a “Type I error”).
- False Negatives (FN): We predicted negative, but actually it is negative (Also known as a “Type II error”).



		Predicted Class	
		Yes	No
Actual Class	Yes	TP	FN
	No	FP	TN

Fig 4: Confusion Matrix

DET (Detection Error Trade off) curves have also been plotted to visualize the performance of fingerprint after using non-invertible transformations. These curves are plotted between False Positive Rate (FPR) and False Negative Rate (FNR) with FPR on x-axis and FNR on Y-axis.

False Acceptance Rate

The false acceptance rate, or FAR measures the probability of incorrectly accepting an unauthorized user. FAR can be calculated as follows:

$$FAR = FP / (FP+TN)$$

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/2RTXH

False Recognition Rate

The false recognition rate, or FRR, measures the probability of incorrectly rejecting an authorized user. FRR can be calculated as follows

$$FRR = FN / (FN+TP)$$

4. RESULTS

4.1 Evaluation Scenario

Evaluation of performance parameters has been done on (i) original feature vectors stored in the form of chain codes and then on (ii) transformed chain codes using XOR and median filter methid for transformations. FVC2004 DB1A [22] database of 1680 images (140 subjects with 12 samples each) is divided as 7 images for training and 5 images for testing.

4.2 Visualizations

Some of the visualizations are –

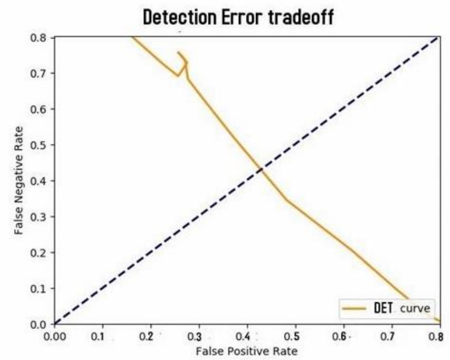


Fig 5 (a): Original case implementation with K-fold crosses validation

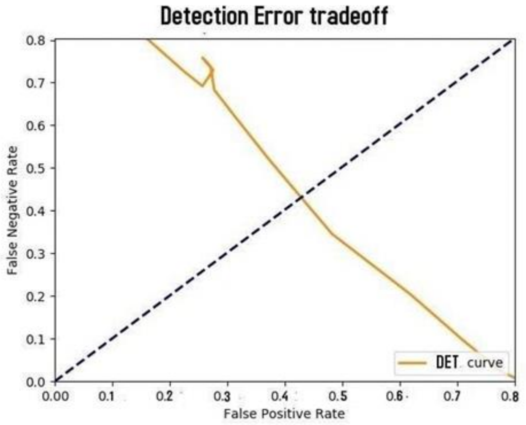


Fig 5 (b): Worst case implementation with K-fold cross validation

DOI 10.17605/OSF.IO/2RTXH

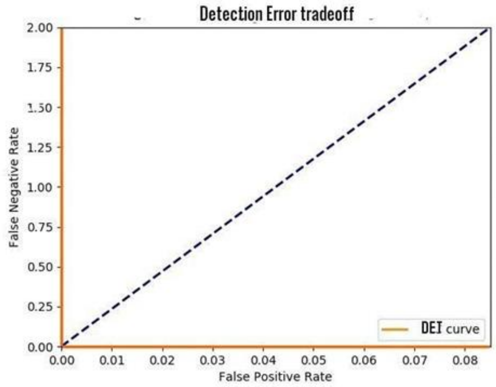


Fig 5(c): Best case implementation with K-fold cross validation

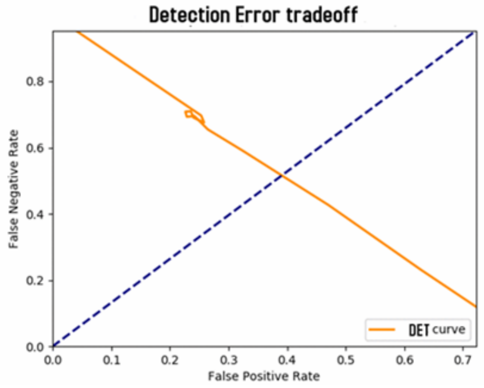


Fig 6 (a): Worst case implementation with K-fold and 5 different Keys (5 Way K-fold)

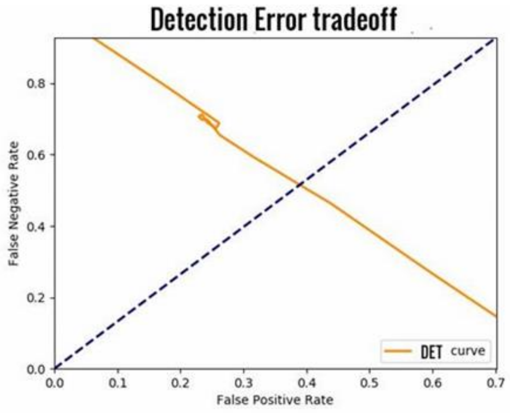


Fig 6 (b): Worst case implementation with K-fold and 10 different Keys (10 Way K-fold)

It is observed that matching is being done with a very high accuracy on the databases as described above (in the section of "Acquisition"). Accuracy and other parameters like False Positive Rate (FPR), False Negative rate (FNR) and True Positive Rate (TPR) have been recorded and visualized on various threshold values.

The efficiency for original feature vector obtained directly from the image in the form of chain codes obtained was 100%.

The efficiency after applying non-invertible transformations to the original feature vector obtained was 100% for both worst and best cases.

Table 1: Equal Error Rate using different methods for different cases

Method/Case	Original Case	Worst Case	Best Case
K-fold	0.42	0.44	0.00
5-way K-fold	-	0.45	0.00
10-way K-fold	-	0.46	0.00

4.3 Comparison Graph

Fig below shows the Accuracy comparison graph of BRISK, SURF and K-Fold algorithms.

Our proposed K-fold cross validation algorithm shows better accuracy compared to those two algorithms.

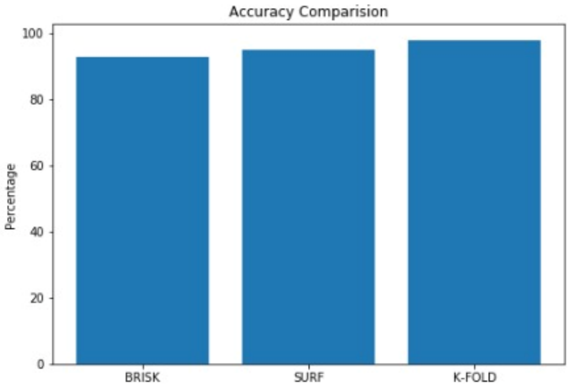


Fig 7: Accuracy Comparison Graph

5. CONCLUSION AND DISCUSSION

After Successfully extraction of dorsal veins and applying non-invertible transformation techniques we are performing training and testing on dataset along with and various performance evaluation parameters show that the templates which generated are non-invertible, we can revoked these templates easily and are performing well. The proposed K-fold cross validation technique based on cancelable biometrics has been tested and it is delivering the good result as compared to the techniques such as SURF and BRISK algorithms which shows less accuracy.

Refrences

1) Xue, M.; Li, J.; Xu, W.; Lu, Z.; Wang, K.; Ko, P.K.; Chan, M. A self-assembly conductive device for direct DNA identification in integrated microarray based system. In Proceedings of the Digest. International Electron Devices Meeting, San Francisco, CA, USA, 8–11 December 2002; pp. 207–210. [Google Scholar]

2) Moreno, B.; Sanchez, A.; Vélez, J.F. On the use of outer ear images for personal identification in security applications. In Proceedings of the IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology (Cat. No. 99CH36303), Madrid, Spain, 5–7 October 1999; pp. 469–476. [Google Scholar]

3) Gao, Y.; Leung, M.K. Face recognition using line edge map. IEEE Trans. Pattern Anal. Mach. Intell. 2002, 24, 764–779. [Google Scholar]

4) Alam, M.; Akhteruzzaman, M. Real time fingerprint identification. In Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No. 00CH37093), Dayton, OH, USA, 12 October 2000; pp. 434–440. [Google Scholar]

5) Lee, C.-S.; Elgammal, A. Gait style and gait content: Bilinear models for gait recognition using gait re-sampling. In Proceedings of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition, Seoul, Korea, 19 May 2004; pp. 147–152. [Google Scholar]

6) Sanchez-Reillo, R.; Sanchez-Avila, C.; Gonzalez-Marcos, A. Biometric identification through hand geometry measurements. IEEE Trans. Pattern Anal. Mach. Intell. 2000, 22, 1168–1171. [Google Scholar] [CrossRef][Green Version]

7) Liam, L.W.; Chekima, A.; Fan, L.C.; Dargham, J.A. Iris recognition using self-organizing neural network. In Proceedings of the Student conference on research and development, Shah Alam, Malaysia, 17 July 2002; pp. 169–172. [Google Scholar]

8) Yu, E.; Cho, S. GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification. In Proceedings of the International Joint Conference on Neural Networks, Portland, OR, USA, 20–24 July 2003; pp. 2253–2257. [Google Scholar]

9) Nakamoto, T.; Moriizumi, T. Odor sensor using quartz-resonator array and neural-network pattern recognition. In Proceedings of the IEEE 1988 Ultrasonics Symposium Proceedings, Chicago, IL, USA, 2–5 October 1988; pp. 613–616. [Google Scholar]

10) Zhang, L.; Zhang, D. Characterization of Palmprints by Wavelet Signatures via Directional Context Modeling. IEEE Trans. Syst. Man, Cybern. Part B (Cybernetics) 2004, 34, 1335–1347. [Google Scholar] [CrossRef] [PubMed][Green Version]

11) Palla, S.; Lei, H.; Govindaraju, V. Signature and lexicon pruning techniques. In Proceedings of the Ninth International Workshop on Frontiers in Handwriting Recognition, Tokyo, Japan, 26–29 October 2004; pp. 474–478. [Google Scholar]

12) Kong, W.K.; Zhang, D. Palmprint texture analysis based on low-resolution images for personal authentication. In Proceedings of the Object recognition supported by user interaction for service robots, Quebec City, QC, Canada, 11–15 August 2002; pp. 807–810. [Google Scholar]

13) Vidhi Bansal, Surabhi Garg, A cancelable biometric identification scheme based on bloom filter and format-preserving encryption, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 8, Part B, 2022, Pages 5810-5821, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.01.014.

14) Wencheng Yang, Song Wang, Muhammad Shahzad, Wei Zhou, A cancelable biometric authentication system based on feature-adaptive random projection, Journal of Information Security and Applications, Volume 58, 2021, 102704, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102704.

15) Pititheeraphab Y, Thongpance N, Aoyama H, Pintavirooj C. Vein Pattern Verification and Identification

ISSN 1533-9211

DOI 10.17605/OSF.IO/2RTXH

Based on Local Geometric Invariants Constructed from Minutia Points and Augmented with Barcoded Local Feature. Applied Sciences. 2020; 10(9):3192. https://doi.org/10.3390/app10093192.

16) D. Chang, S. Garg, M. Hasan, S. Mishra, Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption, IEEE Trans. Inf. Forensics Secur., 15 (2020), pp. 3152-3167.

17) Inshirah Rossan, Maleika Heenaye,"Impact of Changing Parameters when Preprocessing Dorsal Hand Vein Pattern", Procedia Computer Science 32 (2014) Elsevier, pp. 513 – 520, 2015.

18) R. Raghavendra and J.Surbiryala, "Hand Dorsal Vein Recognition: Sensor, Algorithms and Evaluation", IEEE, pp. 4799-8633, January 2015.

19) Yiding wang and Wei Xie, " An Automatic Physical Access Control System Based on Hand Vein Biometric Identification", IEEE Transactions on Consumer Electronics, Vol. 61, No.3, pp. 320-327, August 2015.

20) H. Bay et al., "Speeded-up robust features (SURF)", Computer vision and Image Understanding, vol. 110, no. 3, pp. 346-359, 2008.

21) S. Leutenegger et al., "BRISK: Binary robust invariant scalable keypoints", IEEE International Conference on Computer Vision, pp. 2548-2555, 2011.

22) FVC2004, 2004. Available from: http://bias.csr.unibo.it/fvc2004/databases.asp