УДК 621.396 DOI 10.18522/2311-3103-2020-3-173-183

Шивам Шендре, Шубханги Сапкал

ГИБРИДНЫЙ ПОДХОД К БЕЗОПАСНОСТИ ШАБЛОНОВ БИОМЕТРИЧЕСКИХ ДАННЫХ ВЕН ПАЛЬЦА НА ОСНОВЕ ГЛУБОКОГО ОБУЧЕНИЯ

Мы живем в современном обществе, где у нас достаточно много ресурсов и вычислительной мощности, единственной проблемой остается общественная безопасность. С развитием технологий личная информация становится все более не защищенной. Поэтому идентификация личности является актуальной проблемой. Существующие традиционные методы защиты личной информации оказались не надежными. Защита биометрических параметров является одной из наиболее важных проблем при обеспечении безопасности современной биометрической системы. Имеющиеся алгоритмы не дают адекватного решения этой проблемы. Поэтому мы попытались предложить метод, который будет более актуальным. В этой статье обсуждается гибридный метод биометрического распознавания вен на пальцах, основанный на методе глубокого обучения с использованием схем двоичной диаграммы принятия решений и нечетких обязательств. Предложенный гибридный метод состоит из четырех частей, а именно: извлечение признаков вены пальца, генерация защищенного шаблона, схема нечеткой фиксации, распознавание и принятие решения о структуре вен на пальце. Таким образом, имеются четыре модуля, при этом каждый модуль работает эффективно и дает точные результаты по всем базам данных.

Биометрия, безопасность шаблонов, гибрид, двоичная диаграмма принятия решений (BDD), схема нечетких обязательств, глубокое обучение и машинное обучение.

Shivam Shendre, Dr. Shubhangi Sapkal

A HYBRID APPROACH FOR DEEP LEARNING BASED FINGER VEIN BIOMETRICS TEMPLATE SECURITY

We are living in the today's society, where we have fairly-enough storage capacity and processing power, the only issue is with security. As, the technologies are evolving with faster rate, we are tend to grow the use of electronic devices rapidly in todays' society, it started to flow or leakage of personal information around/across, which then leads to breach of this information. Now, personal or identical verification is key problem is being crucial. So whatever traditional methods we have for providing authentication or security those have proven inadequate to be unreliable and do not provide strong security. Biometric template protection is one of the most important issues in securing today's biometric system. We have many algorithms which don't give adequate solution for the same. So we tried to give a method which will reach to the expectations more satisfactorily and certainly to the extent required. In this paper we have discussed a hybrid method for finger vein biometric recognition based on deep learning approach using BDD and fuzzy commitment schemes. The proposed hybrid method consists of four parts, namely Finger vein feature extraction, BDD-based secure template generation, Fuzzy commitment scheme and ML based finger vein recognition and decision making. Thus it has four module and each module works efficiently and gives accurate results on all databases.

Biometric, template security, hybrid, binary decision diagram (BDD), fuzzy commitment scheme, deep learning and machine learning

Introduction. Biometric recognition is a reliable, robust, and convenient way for person authentication with growing concerns about security and terrorism, several large-scale biometric systems. Biometric systems are also being developed for many other applications such as banking (for ATM machines), the credit card industry, and physical access control. With the growing use of biometrics, there is a rising concern about the security and privacy of the biometric data itself. Since each person is claimed to have a unique biometric (e.g., fingerprint, face, and iris), if this biometric data is compromised,

it is impossible to have a replacement. Therefore, biometric data (template) security is one of the most important issues in developing a practical biometric system [2] (biometric template refers to the extracted biometric features stored in a central database or a smartcard). Edge computing, which refers to data processing at the edge devices of a network, has become the latest computing paradigm for reducing latency and achieving real-time services.

Every second, massive amounts of data are created by billions of Internet of Things (IoT) devices. Although cloud servers own super-powerful service ends and have a fast data processing speed, data transportation has become a bottleneck. Also, unnecessary bandwidth costs are high if tremendous volumes of raw data are exchanged between end users and the cloud server [1]. Authentication is the act of confirming the truth of an attribute of a datum or entity. The process of identifying an individual usually based on a username and password. There are different types of techniques used for authentication like personal identification number (PIN), Key smartcards, Deoxyribonucleic acid (DNA), Face recognition, fingerprint, iris ,voice recognition etc. now a day these methods do not provide adequately strong security. Hence, personal verification methods that utilize a person biometric trait has been intensively investigated and developed to overcome the disadvantage of the traditional methods. Biometric recognition (biometrics) refers to automatic recognition of individual based on their physiological and behavioral characteristics. Many biometric such as face, fingerprint, is and voice have been developed [19].

There are many applications of edge biometrics with AI. We give three examples in [1]. 1) Automated surveillance: Smart cameras with built-in AI capabilities can figure out whom they are see inland track specific individuals; 2) Gait identification: By using specific sensors on a mobile device, a person‘s way of walking can be identified by AI algorithms. With rapid evolution of on-device AI algorithms, higher identification accuracy using gait will be achievableint he foresee able future. 3) Voice authentication/assistant: Nowadays, smart phones with voice assistant powered by AI, e.g., Siri on iPhone, are commonplace. Vein patterns are the vast network of blood vessels underneath a person’s skin. They are unique to each individual and are stable over long period time. It provides “aliveness” detection as it senses the flow of blood in the vessels. Even twins are said to have different finger vein patterns. It is used in hospitals, law enforcement, military facilities and other applications that require very high levels of security. Vein recognition biometric devices can also be used for PC login, bank, ATM identification, verification, and many other applications such as opening car doors. Vein recognition biometrics is a particularly impressive and promising technology because it requires only a single-chip design, meaning that the units are relatively small and cheap. Using alight transmission technique, the structure of the vein pattern can be detected, captured and subsequently verified [20].

Although biometric security for non-machine learning based finger vein recognition systems is an established topic; there is a major security loophole in the existing machine/deep learning based finger vein identification systems, which do not protect raw finger-vein templates. This security issue is particularly crucial given the fact that artificial neural networks for image classification are invertible. A novel biometric tem- plate protection algorithm using the binary decision diagram (BDD) [4] for deep learning based finger vein biometric systems. Specifically, instead of using raw finger-vein templates for biometric recognition, a transformed version of the raw finger-vein template is created by a noninvertible transformation based on the BDD. The transformed version is further processed by a multilayer extreme learning machine (ML-ELM) for training and classification. Thanks to template protection, the deep learning based privacy preserving finger vein recognition system named BDD-ML-ELM has heightened security [1].

In this paper, we investigate a methods on non-deep learning base and deep learning based finger vein authentication and recognition and propose new hybrid algorithm with high performance and optimum accuracy. The rest of the paper is organized as follows. Section IV describes the proposed system.

Related work. Finger-vein based biometric recognition has come in use more drastically in the past few years. Finger-vein recognition is widely divided into two types, (1) Non-machine learning based and (2) Machine-learning based.

In [1, 3], Miura et al. proposed to use repeated line tracking to extract finger-vein features from an unclear finger-vein image. The line tracking operation starts from different positions and is repeated multiple times. In order to handle challenges brought by noise and deformation, in [5], Gupta et al., proposed alow-cost finger-vein sensor based on a single camera that can capture finger-vein images from dorsal and ventral parts of the finger with high quality, system consists of multiple near- infrared light sources to illuminate the finger from both sides and top, coupled with the custom designed physical structure to facilitate high reflectance of the emitted light and distribute the light uniformly on the finger to capture good-quality dorsal and ventral finger-vein patterns. Extensive experiments are carried out on the data captured using the developed sensor and benchmarked the performance with eight different state- of-the-art (SOTA) algorithms.

In [6], Xi et al. proposed a novel discriminative binary codes (DBC) learning method for finger vein recognition, in which the subject relation graph is built to capture correlations among subjects and binary templates are transformed to describe vein characteristics of subjects then graph transform is formulated into an optimization problem, in which the distance between templates from different subjects is maximized and templates provide maximum information about subjects and finally supervised information for training instances is provided by the obtained binary templates, and SVMs are trained as the code learner for each bit. In [7], Lu et al. proposed a system for finger vein recognition, including an anatomy structure analysis-based vein extraction algorithm and an integration matching strategy in which pattern is extracted from the orientation map-guided curvature and it is further refined to obtain a network finally the similarity matches by elastic matching and recomputed by integrating the overlap degree of veins. In [8], Kauba et al. made a strategyie the fusion of several feature extractors' outputs, and the study involving different feature extraction techniques (maximum curvature, repeated line tracking, wide line detector, ...) and different fusion techniques (majority voting, weighted average, STAPLE, ...) on multiple finger vein datasets.

In [9], Liu and Kim defined an efficient finger-vein extraction algorithm based on random forest training and regression with efficient local binary pattern feature. They achieved state- of-the-art finger vein recognition by integrating the vein pattern matching method, which is robust to finger misalignment. In [10], Van et al., discussed method to improve the performance of finger vein identification systems includes three steps first, images of finger veins are cropped to have regions of interest (ROI's) then, local invariant orientation features are extracted by using MFRAT and then, Grid PCA is applied to further remove redundant information and form a discriminant representation finally, the enlarging training set (ETS) based matching technique is used to overcome the translations. In [11], Banerjee et al. developed a finger vein based biometric authentication system by combining three algorithms–an image enhancement algorithm, a registration algorithm based on mutual information and affine transformation, and a matching algorithm based on correlation coefficient.

As we are going work on deep learning based approach, our main focus or aim to AI, machine learning or deep learning and it has achieved promising results in tasks, such as speech, image, and video processing, as well as, biometric recognition, e.g., finger vein image recognition. In [1], they proposed an algorithm which is capable of creating a new

noninvertible version of the original finger-vein template, which is stacked with an artificial neural network– the multilayer extreme learning machine (ML-ELM) to generate a privacy-preserving finger-vein recognition system i.e. named BDD-ML-ELM.

In [12], a four-layer convolutional neural network (CNN) with the convolutional-subsampling architecture is designed, for finger-vein recognition. In this scheme, a modified stochastic diagonal Levenberg–Marquardt algorithm is utilized to network training to make convergence faster. In [13], proposed a finger-vein recognition method which is robust to the three database that they used and environmental changes based on the convolutional neural network (CNN) by using NRI image sensor. In [14], for finger-vein verification, a deep learning based segmental model is developed to predict the probability of pixels from veins or the background. Moreover, a missing finger vein pattern recovering method based on a fully convolutional network is introduced to improve recognition performance. Das et al., [15] proposed a deep learning based scheme to handle finger-vein images of varying qualities. In [15], extensive experiments are conducted on four different publicly available databases to evaluate system performance. A lightweight deep learning scheme for finger-vein verification is proposed in [16], which tackles the restrictions of CNN, e.g., large training sample sizes and high computation. The proposed scheme contains a two-channel convolutional net- work to solve the problem of a lack of finger-vein data, while demonstrating satisfactory performance. The extreme learning machine (ELM) [17], as a kind of artificial neural network, is another stream of AI. In an ELM, the hidden layer biases and input weights are randomly assigned without requiring any fine-tuning of parameters, making it much faster than a traditional deep learning neural network, e.g., CNN. Therefore, it is attracting a strong research interest in image classification and regression, including finger vein recognition. For example, in [18], the feature component based ELMs are designed to improve recognition accuracy and stability. Features are extracted from eight block based directional features. The extracted features are further trained by eight single ELMs and the outputs of the eight ELMs are connected by an output layer before classification is performed.

Motivation and objective. After knowing the Consequences and the risk of biometric data breach and this could be used in a wide range of criminal activities that would be disastrous for both the businesses and the organizations, also equally can affect, as well as their employees and clients/associates.

With the rapid growth and use of electronic information systems in today's society, personal or identity, verification is now a critical key problem. Traditional method uses personal identification number (PIN), password, key smartcards, etc. But these methods have proven adequately to be unreliable and do not provide strong security. So, the biometrics, which are highly accurate and use a part of one's body, have become the ideal answer to these security needs [20]. The advancement of on-device AI will undoubtedly accelerate the development of voice recognition technique.

With the rapid development of AI, machine learning based biometric recognition systems are advantageous to their non-machine learning counterpart due to superior recognition performance. However, given that deep learning methods, e.g., CNN, being a representative of AI, are invertible using the outputs from the trained network, machine learning based biometric systems may suffer security threats, such as adversaries retrieving raw biometric templates by inverting the artificial neural network. This information leakage is a considerable security weakness of machine learning based biometric recognition [1].

The only objective of this paper is to propose a hybrid technique of finger vein recognition based on the deeplearning approach, which will be more accurate and faster than the existing methods.

Proposed hybrid approach. As we mentioned in the section III the motivation behind. In this section we are going to discuss the detail structure and technique of proposed system. The deep learning base hybrid system with template security mainly consists of four parts as they follows: Finger vein feature extraction, BDD-based secure template generation, Fuzzy commitment scheme and ML based finger vein recognition and decision making. AS you can see in Fig. 1.

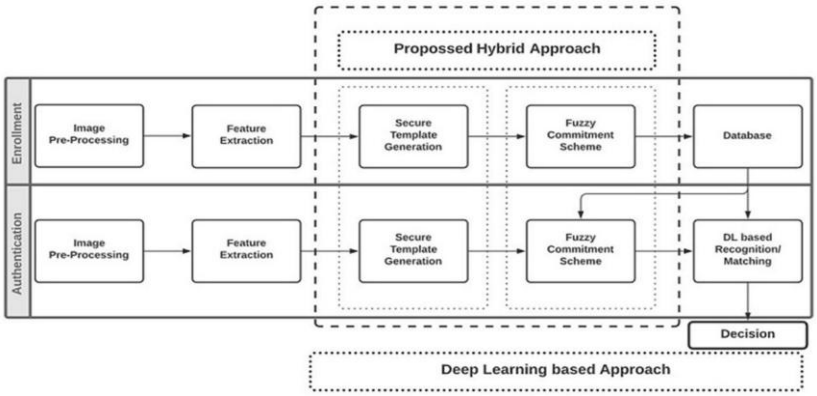

Fig. 1. Block diagram of the proposed hybrid system

A. Finger Vein Feature Extraction

This operation will perform for both the Enrolment as well as Authentication part. First take the image and perform the pre-processing operation in it later give an input finger- vein image, region of interest (ROI) extraction and image enhancement should be performed first. After ROI extraction and image enhancement using the same methods as in [18].

The enhanced finger-vein image is further processed by a set of Gabor filters and the linear discriminate analysis (LDA) [23]. Finger vein's texture features and characteristics provide information about the spatial arrangement of color or intensities of a finger-vein image. These features are extracted by a filter bank at different orientations and on different scales. The filter bank contains 40 Gabor filters of eight orientations and five scales, using the same parameter settings in [23] for finger-vein texture feature extraction. The texture featurevectorextractedfromafinger-veinimageofsize256 × 96 with the constructed Gabor filter bank is of super high dimension, which is costly to process and store. Hence, the dimensionality reduction technique, LDA [23] is employed to reduce the feature vector's dimension. By this means, a real- valued feature vector FR of length NR is created.

B. BDD-Based Secure Template Generation

In this step, Adapted from [1] BDD-based noninvertible transformation and apply it to the binary vector FB to generate secure finger-vein templates. Since both the inputs and outputs of the proposed transformation are binary vectors, only Boolean operation is needed, for which the BDD [4] is a good fit. We design a BDD with three variables, b1, b2, and b3. As shown in Fig. 2, the designed BDD has a structure of b1 being the root, and b2 and b3 being the decision nodes. Each decision node, b2 or b3 has two child nodes named low child and high child. In Fig. 2, the dotted line (labelled 0) represents the path to the low child, while the solid line (labelled 1) denotes the path to the high child. Now combine the BDD (as shown in Fig. 2) and the permutation technique to produce a noninvertible transformation, which is to be used to generate a cancellable finger-vein template with strong security. Then the transformed feature vector FB will serve as the input to the subsequent deep-learning algorithm.

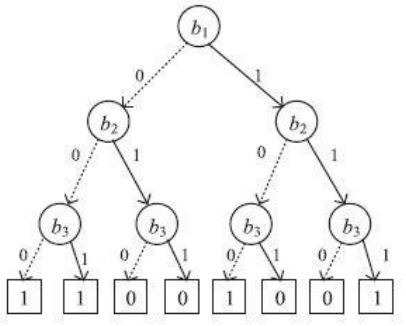

Fig. 2. Designed BDD (adapted from [4])

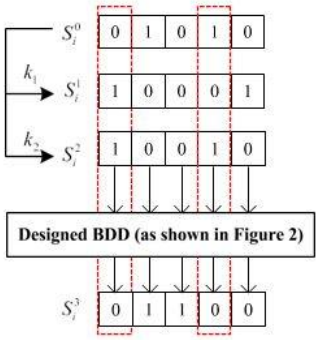

Fig. 3. Example of the BDD-based transformation

We give a simple example to illustrate the above-mentioned BDD-based transformation. Assume that the original segment S^0=`01010' and the user-specific keys are k_1= [4,3,1,5,2] and k_2 = [2, 1, 5, 4, 3]. Under the guidance of k_1 and k_2, two new segments are generated as S^1=J10001J and S^2=J10010J, respectively. If the variables b_1, b_2, and b_3 in the BDD are, respectively, as signed the first element of S^0, S^1 and S^2,i.e., b_1= 0, b_2= 1 and b_3= 1, then according to the designed BDD in Fig. 2, the output is $f(b_1$= 0, b_2= 1, b_3= 1)=0, as indicated in the first red rectangle in Fig.3.I fb_1=1, b_2=0, and b_3=1 are as signed, as shown in the second red rectangle in Fig. 3, then the output is $f(b_1$= 1, b_2= 0, b_3= 1) is also 0. After applying this operation to all three segments element by element, we get a new binary segment S^3. By concatenating all the new segments, transformed from F_B by the designed BDD and permutation, we form a new feature vector $F_{B,}$ which is the secure finger-vein template [1].

C. *Fuzzy Commitment Scheme*

In [2], they explained a fuzzy commitment scheme which treats the biometric template itself as a corrupted code word. The security of this method is linked to the number of code words. The scheme encrypts the original template u_E to a pair (Hash C) where C is a randomly generated code word. At authentication, given a query template u_A, the method computes result and corrects it to the closest code word C^1. If u_E is close to u_A then will be corrected to C, (i.e. C^1 = C). Then Hash (C^1) and Hash(C) are compared to make the decision. This algorithm can tolerate a relatively large error rate with enhanced security level. Also, both the off-line scheme and the fuzzy commitment scheme require a binary input.

D. ML-ELM-Based Finger-Vein Recognition

Extreme learning machines are feedforward neural networks with a single layer or multiple layers of hidden nodes, where the parameters of hidden nodes (not just the weights connecting inputs to hidden nodes) need not be tuned. These hidden nodes can be randomly assigned and never updated (i.e. they are random projection but with non-linear transforms), or can be inherited from their ancestors without being changed. In most cases, the output weights of hidden nodes are usually learned in a single step, which essentially amounts to learning a linear model. In most cases, ELM is used as a single hidden layer feedforward network (SLFN) including but not limited to sigmoid networks, RBF networks, threshold networks, fuzzy inference networks, complex neural networks, wavelet net- works, Fourier transform, Laplacian transform, etc. Due to its different learning algorithm implementations for regression, classification, sparse coding, compression, feature learning and clustering, multi ELMs have been used to form

multi hidden layer networks, deep learning or hierarchical networks. A hidden node in ELM is a computational element, which need not be considered as classical neuron. A hidden node in ELM can be classical artificial neurons, basis functions, or a subnet work formed by some hidden nodes. Here we used to make our system faster than traditional systems in terms of accuracy and computing.

The ML-ELM possesses a multilayer learning architecture that stacks single ELMs one by one in a hierarchical structure, as demonstrated in Fig. 4(a). In our method, the secure template feature vector F_B, generated from the previous step, is treated as the input to the ML-ELM. The output of the $(k\text{-}1)^{th}$ hidden layer is used as the input to the k^{th} hidden layer. Similar to traditional deep neural networks, the hidden layer weights β_{k-1} of the $(k\text{-}1)^{th}$ hidden layer are initialized by using ELM auto encoder, but the time for fine tuning is not required. The ELM auto encoder performs layer wise unsupervised training that uses the inputs as outputs with the traditional least mean square method to compute the hidden layer weights β_{k-1}, as shown in Fig. 4(b). By going through the above-mentioned recursive calculation, the ML-ELM with N_H hidden layers out-puts a vector O containing the probability values for all the available classes/subjects. The maximum probability indicates the most similar class/subject that the test sample belongs to [1].

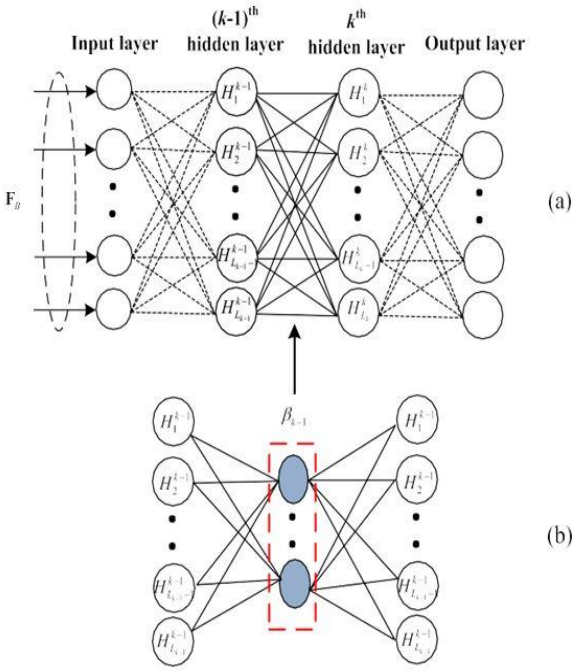

Fig. 4 (a). Structure of the ML-ELM and (b) the ELM auto encoder

Experimental results. In the experimental results section, we divided results into three parts. Part I, reports the image pre-processing and enhancement using Gabor filter and guided filter. The accuracy of the proposed hybrid algorithm is evaluated and reported in Part II. The decision making of the hybrid algorithm is discussed in Part III.

The public domain database is used in our experiment, first of all we found ROI (Region of Interest) from the give input image as shown in following image.

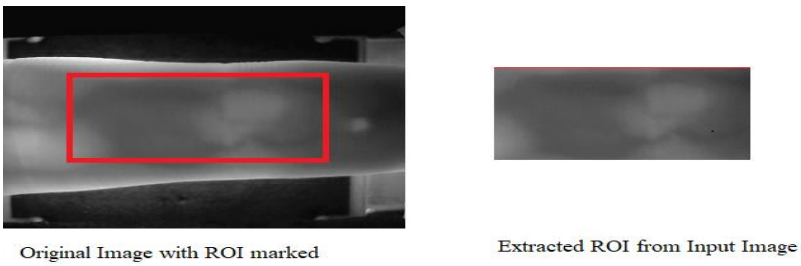

Fig. 5. Extraction of ROI from Input image

The proposed image pre-processing method comprises of eight sub-steps: color to grayscale conversion, grayscale median filter, image alignment and resize, global thresholding, Adaptive mean thresholding, Gaussian thresholding, and lastly thinning process. The result is shown in Fig. 6 and Fig. 7.

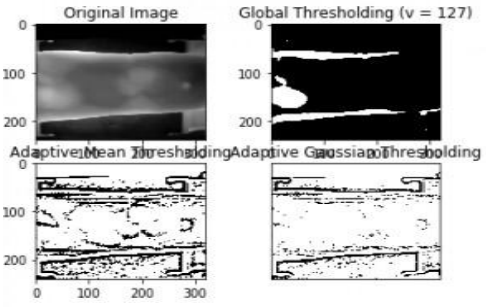

Fig. 6. Output images after applying thresholding

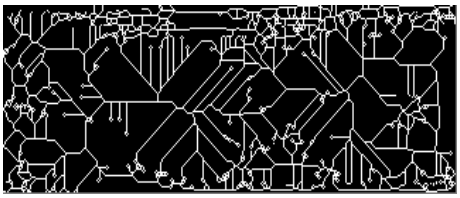

Fig. 7. Output images after Thinning

Then after extracting features from the input image, we further pass these from BDD (Binary Decision Diagram to generate the secure template, as the output we get new feature vector containing encrypted new feature data.

To further increment of security we again apply the Fuzzy Commitment Schemes to the output vector and generate new highly secure template vector with new encrypted and secure feature for the same input image and stored in the Database with a particular key.

All modules of this system working very efficiently on each image of given dataset of finger vein images. And performing cancelability and discriminability and increasing security.

Experiment was carried out to evaluate the performance of the system in term of speed and accuracy. Preliminary experiment on our finger vein database consists of 3816 images from 106 person'sfingers. The system working properly on the given database and giving overall accuracy of 93 % as a result.

The testing accuracy, measured by the correct identification rate (CIR), is plotted in Fig. 8, from which we can see that, it provides strong template protection to the proposed deep learning based finger vein recognition system. Indeed, it is a balance between recognition accuracy and security.

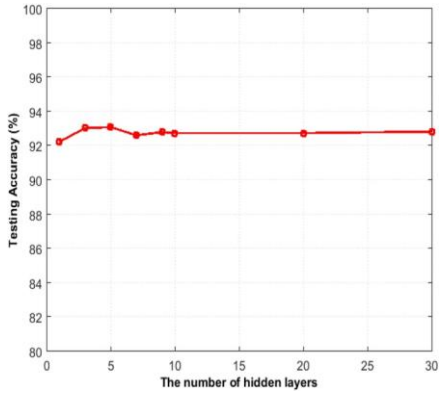

Fig. 8. Testing accuracy against hidden layers

Conclusion. The primary focus of this paper is to enhance the security of the pattern for finger vein authentication system as we are living in the era where we don't have problem of storage space and processing capability. So here we proposed the hybrid approach takes advantage of deep leaning based finger vein recognition system and fuzzy commitment scheme. The proposed framework consists of four parts, namely Finger vein feature extraction, BDD-based secure template generation, Fuzzy commitment scheme and ML based finger vein recognition and decision making.. Each part provides the template cancellable ability, discriminability, and security, respectively. The proposed system is an enhancement over most existing permutation based cancellable biometrics as well as machine learning based finger vein recognition systems, which offer no template protection. And accurate up to 93 %. And all modules in proposed model are working efficiently.

For future work on this system, work continues on the investigation on hoe to improve recognition accuracy and application of this method on the multiple databases and performance accuracy on those databases. Given below we have table showing, the comparison of proposed system with some other existing systems.

Table 1

Performance comparison in CIR

Methods	Template Protection	Accuracy (CIR)
Van et al. [10]	No	95.67%
Xie et al. [18]	No	97.76%
Banerjee et al. [11]	No	90.72%
Miura et al.[3]	No	96.06%
Das et al.[15]	No	98.90%
Kauba et al.[8]	No	-
Fang et al.[16]	No	90.47%
Liu and Kim [9]	No	-
Hong et al. [13]	No	93.91%
Yang et al. [1]	Yes	96.21%
Proposed Hybrid Method	Yes	93.05%

REFERENCES

1. *Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, Jucheng Yang, and Craig Valli.* Securing Deep Learning Based Edge Finger Vein Biometrics With Binary Decision Diagram, *IEEE Trans. on Industrial Informatics*, July 2019, Vol. 15, No. 7, pp. 4244-4253.
2. *Yi C. Feng, Pong C. Yuen, and Anil K. Jain*. A Hybrid Approach for Generating Secure and Discriminating Face Template, *IEEE Tansactions on Information forensics and security*, March 2010, Vol. 5, No. 1, pp. 103-117.
3. *Miura N., Nagasaka A., and Miyatake T.* Feature extraction of fingervein patterns based on repeated line tracking and its application to personal identification, *Mach. Vision Appl.*, Oct. 2004, vol. 15, pp. 194-203.
4. *Akers S.B.* Binary decision diagrams, *IEEE Trans. Comput*. Jun. 1978, Vol. C-27, No. 6, pp. 509-516.
5. *Gupta P. and Gupta P.* An accurate finger vein based verification system, *Digit. Signal Process*, 2015, Vol. 38, pp. 43-52.
6. *Xi X., Yang L., and Yin Y.* Learning discriminative binary codes for fingervein recognition, *Pattern Recognit*, 2017, Vol. 66, pp. 26-33.
7. *Yang L., Yang G., Yin Y., and Xi X*. Finger vein recognition with anatomy structure analysis, *IEEE Trans. Circuits Syst. Video Technol*., Aug. 2018, Vol. 28, No. 8, pp.1892-1905,.
8. *Kauba C., Piciucco E., Maiorana E., Campisi P., and Uhl A.* Advanced variants of feature level fusion for finger vein recognition, *Proc. Int. Conf. Biometrics Special Interest Group*, 2016, pp. 195-206.
9. *Liu C. and Kim Y.-H.* An efficient finger-vein extraction algorithm based on random forest regression with efficient local binary patterns, in Proc. IEEE Int. Conf. Image Process, 2016, pp. 3141-3145.
10. *Van H.T., Thai T.T., and Le T.H*. Robust finger vein identification base on discriminant orientation feature, in Proc. 7th Int. Conf. Knowl. Syst. Eng., 2015, pp. 348-353.
11. *Banerjee A., Basu S., Basu S., and Nasipuri M.* ARTeM: A new system for human authentication using finger vein images, *Multimedia Tools Appl*., 2018, Vol. 77, pp. 5857-5884.
12. *Radzi S.A., Hani M.K., and Bakhteri R*. Finger-vein biometric identification using convolutional neural network, *Turkish J.Elect.Eng. Comput. Sci.*, 2016, Vol. 24, pp. 1863-1878.
13. *Hong H.G., Lee M.B., and Park K.R.* Convolutional neural network- based finger-vein recognition using NIR image sensors, Sensors, 2017, Vol. 17, pp. 1297.
14. *Qin H. and El-Yacoubi M.A.* Deep representation-based feature extraction and recovering for finger-vein verification, *IEEE Trans. Inf. Forensics Security*, Aug. 2017, Vol. 12, No. 8, pp. 1816-1829.
15. *Das R., Piciucco E., Maiorana E., and Campisi P*. Convolutional neural network for finger-vein-based biometric identification, *IEEE Trans. Inf. Forensics Secur*., Feb. 2019, Vol. 14, No. 2, pp. 360-373.
16. *Fang Y., Wu Q., and Kang W.* A novel finger vein verification system based on two-stream convolutional network learning, *Neurocomputing*, 2018, Vol. 290, pp. 100-107.
17. *Huang G.-B., Zhu Q.-Y., and Siew C.-K*. Extreme learning machine: theory and applications, *Neurocomputing*, 2006, Vol. 70, pp. 489-501.
18. *Xie S.J., Yoon S., Yang J., Lu Y., Park D.S., and Zhou B*. Feature component-based extreme learning machines for finger vein recognition, *Cogn. Comput*., 2014, Vol. 6, pp. 446-461.
19. *Khalil-Han M. and Eng P.C*. FPGA-Based embedded system implementation of finger vein biometrics, *IEEE Symposium on Industrial Electronics and Applications (ISIEA 2010), October 3-5, 2010, Penang Malaysia*.
20. *Ayappan G. and Shankar A.* Finger Vein biometric Authentication System, *International Journal of Trend in Research and Development*, April 2017, Vol. 4 (2), pp. 51-53.
21. *Yang W., Hu J., and Wang S.* A finger-vein based cancellable bio- crypto system, i*n Proc. Int. Conf. Netw. Syst. Secur.*, 2013, pp. 784-790.
22. *Yang W., Wang S., Hu J., Zheng G., and Valli C*. A fingerprint and finger-vein based cancelable multi-biometric system, *Pattern Recognit.*, 2018, Vol. 78, pp. 242-251.
23. *Yang W., Hu J., Wang S., and Yang J.* Cancelable fingerprint templates with Delaunay triangle-based local structures, *in Proc. Cyberspace Safety Secur.: 5th Int. Symp.*, 2013, pp. 81-91.
24. *Vitomirand S., Nikola P.* The complete Gabor-Fisher classifier for robust face recognition, *EURASIP J.Advances Signal Process.*, 2010, Vol. 2010, Art. no. 31.

25. *Jin A.T.B., Ling D.N.C., and Goh A.* Bio hashing: Two factor authentication featuring finger print data and tokenised random number, *Pattern Recognit.*, 2004, Vol. 37, pp. 2245-2255.
26. *Kasun L.L.C., Zhou H., Huang G.-B., and Vong C.M*. Representational learning with extreme learning machine for big data, *IEEE Intell. Syst.*, Dec. 2013, Vol. 28, No. 6, pp. 31-34.

Статью рекомендовал к опубликованию д.т.н., профессор И.Б. Аббасов.

Шивам Шендре – Государственный инженерный колледж Аурангабада, Университет Маратвады им. доктора Бабасахеба Амбедкара; e-mail: shivamshendre8411@gmail.com; Аурангабад - 431005, Махараштра, Индия, тел.: +918623082270; кафедра компьютерных наук и инженерии; магистр технологий.

Доктор Шубханги Сапкал – e-mail: shubhangisapkal24@gmail.com; тел.: +919922112410; кафедра компьютерных наук и инженерии; доцент.

Shivam Shendre – Government College of Engineering Aurangabad, Dr. Babasaheb Ambedkar Marathwada University; e-mail: shivamshendre8411@gmail.com; Aurangabad - 431005, Maharashtra, India, phone: +918623082270; the department of comp. sci. & engineering; cand. of master of technology.

Dr. Shubhangi Sapkal – e-mail: shubhangisapkal24@gmail.com; phone: +919922112410; the department of comp. sci. & engineering; assistant professor.