Soft Comput (2018) 22:2257–2265
https://doi.org/10.1007/s00500-017-2487-9

METHODOLOGIES AND APPLICATION

Finger vein secure biometric template generation based on deep learning

Yi Liu[1] · Jie Ling[1] · Zhusong Liu[1] · Jian Shen[2] · Chongzhi Gao[3]

Published online: 21 January 2017
© Springer-Verlag Berlin Heidelberg 2017

Abstract Leakage of unprotected biometric authentication data has become a high-risk threat for many applications. Lots of researchers are investigating and designing novel authentication schemes to prevent such attacks. However, the biggest challenge is how to protect biometric data while keeping the practical performance of identity verification systems. For the sake of tackling this problem, this paper presents a novel finger vein recognition algorithm by using secure biometric template scheme based on deep learning and random projections, named FVR-DLRP. FVR-DLRP preserves the core biometric information even with the user's password cracked, whereas the original biometric information is still safe. The results of experiment show that the algorithm FVR-DLRP can maintain the accuracy of biometric identification while enhancing the uncertainty of the transformation, which provides better protection for biometric authentication.

Keywords Secure biometric template · Random projection · Deep belief network

Communicated by V. Loia.

✉ Yi Liu
yiliu@gdut.edu.cn

Jie Ling
jling@gdut.edu.cn

Zhusong Liu
liuzs@gdut.edu.cn

[1] School of Computer Science and Technology, Guangdong University of Technology, Guangzhou, China

[2] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China

[3] School of Computer Science, Guangzhou University, Guangzhou, China

1 Introduction

The omnipresent Internet has provided us an increasing series of services, like entertainment, study, financial transaction. With the development of information technology, the communication between people has become more convenient and faster. People from different areas can communicate and share their sensitive resource on the Internet. This trend certainly will add rise to the problems of data leaks caused by the use of fake identification. In authentication technology, how to authenticate the identity automatically, quickly and accurately is crucial to solve above problems.

The ownership, knowledge and inherence factors (Pankanti et al. 2000) are three different elements to make identity authentication. The password-based knowledge is the traditional authentication method which has been used for several decades. However, this method has shortcomings: The password can be forgotten, attacked and leaked easily.

Biometric identification technology has advantages over above traditional method, since each person's biological characteristic is unique and difficult to counterfeit. The biological characteristics are classified into two types: physiological characteristics and behavioral characteristics. Physiological features include finger vein, palm, iris. Behavior characteristics include signature, speech, gait. At present finger vein recognition is an ideal identification technology. This technology has the following advantages: (1) Each person's finger vein is unique, i.e., every human being has a different finger vein. (2) Each person's finger vein is quite fixed. It will not change throughout a human being's life. (3) A person's finger vein is easy to be sampled. (4) The template used in the identification system is not the original finger vein image but the feature of the image. Thus, the storage and transmission can be minimized.

Most of traditional finger vein identification systems use a template in the form of bare data to store the finger vein information. Thus, the entire finger vein recognition system is likely to be completely exposed to the hacker attacks, which will make the biometric templates unsafe when it needs to store and transmit (Uludag et al. 2004). In this paper, we focus on the need for mechanisms guarding the user's privacy with the help of biometric authentication. The secure storage system of users' authentication templates should be robust and accessible (Rua et al. 2012; Kong et al. 2008). In detail, we have the following requirements:

Security: Keeping the original authentication and the user-specific factors is the primary task of the secured template. Even when his/her data are matched with other users, the privacy of the data should wholly intact.

Performance: When secure template is added to user authentication system, the performance must not seriously depress in comparison with other non-secured counterparts. Moreover, false reject rate (FRR) and false accept rate (FAR) should still stand the low level.

Renewability: The secured template and the user-specific factors should be revocable for the sake of compromise. If a valid authentication data are provided, then a new unparalleled template can be created.

To meet above requirements, we present a framework for template generation, which forecasts biometric data randomly and uses secret key to create a more reliable, efficient and unique biometric templates for identity verification. On the server side, the framework uses deep belief networks as the verification algorithm. The key feature of this scheme FVR-DLRP (random projections and deep belief network) can effectively ensure the security of user data without leakage, because of the complexity of the structure of deep belief networks. In addition, the framework performs multifactor authentications requiring biometric data and correcting user-specific password.

The paper is organized as follows. Section 2 reviews relevant work related to biometrics security. Section 3 explains the tradition biometric template generation schemes and discusses its disadvantages. In Sect. 4, we introduce our constructions for the FVR-DLRP scheme. In Sect. 5, the evaluation of the proposed framework is presented. Finally, we draw a conclusion and make a general summary of the future research direction.

2 Related works

Vein recognition technology is one of the highly reliable identity authentication methods, and scholars who study it are in increasing number due to its good specificity, uniqueness and hardness to be forged. As the second generation of biometric authentication technology, the finger vein recognition has become more popular and acceptable because of its outstanding advantages (Wang et al. 2013). Finger vein recognition is a kind of feature recognition technology of living creatures, and it draws enough attention in many fields, like biometric key (Li et al. 2015a; Wu et al. 2016a), hybrid cloud security (Li et al. 2015b), attribute-based encryptions (Li et al. 2013; Gu et al. 2014; Shen et al. 2015). Liu et al. (2010) presented a straight-forward matching algorithm about the template: First, an appropriate threshold obtained by experiment is set. Then the comparability between the test ones and the stored finger pictures is calculated. Lastly, compare the threshold and the calculated similarity. Only when the similarity is greater than the threshold, it can be considered that those two figures are matched and vice versa. Owing to the incomplete coordinate matching method, this process may be not efficient all the time. Li et al. (2007) extracted the features of the finger vein by using the invariant matrix, then judged the similarity between the test and training data through Hausdorff distance (HD) algorithm. The method combining principal component analysis (PCA) and linearity distinction analysis (LDA) proposed by Wang (2007) can increase the accuracy rate on the single feature recognition. The above matching methods all have large computational cost.

A series of recent works focused on protecting the biometric data in the form of templates. These schemes roughly can be divided into two categories: biometric cryptosystems and feature transformation schemes (Jain et al. 2005). In biometric cryptosystems, user's identification can be proofed by the generated data. And during enrollment and verification process, it use error-correcting codes to handle the intra-user variability of templates (Lim et al. 2012). Biometric cryptosystems have a good performance as preserving the inter-user variability (Maiorana 2010). But it is difficult to generate renewable templates in these systems. In feature transformation techniques, a transformation function should be applied to the original biometric data, which depends on a randomly generated user-specific key. Based on the above points, the feature transformation techniques present a good revocability. In this framework, Ratha et al. (2001) put forward a conceptual design of revocability biometric template for the first time. Many researchers have followed their work and proposed a variety of ways to construct the revocable template, which can be roughly divided into the following types:

- Simple transformation method: Ang et al. (2005) proposed a method that feature image template uses feature points which is difficult to extract. But because of the positioning accuracy problem and reliability problems, the matching accuracy is not satisfied. In addition, there is no change in the detail feature point, which provides a reliable source of original data for attackers.
- Bio hashing method: Maio and Nanni (2005) proposed a two-factor authentication method based on combination

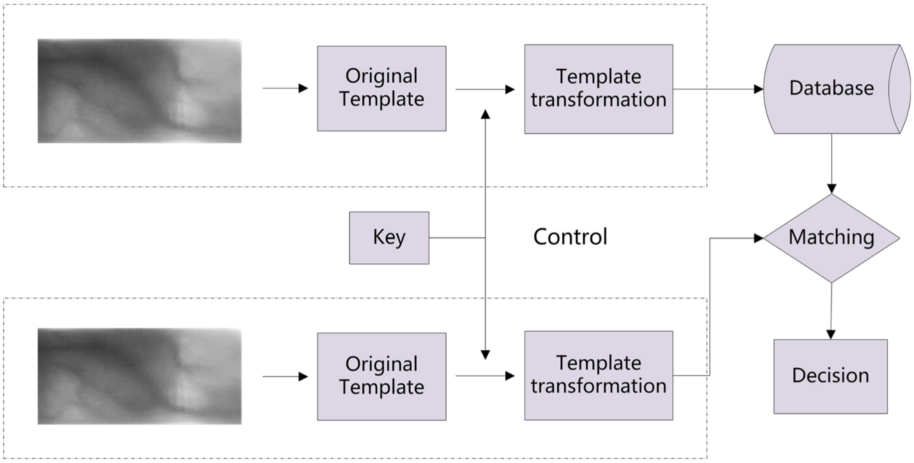


Fig. 1 Traditional schemes of biometric template generation

of biometric data and random key. Using random key rather than the biometric data, this method has a better performance than methods using single biometric data. Nanni and Lumini (2008) improved the method by using stochastic subspace and achieved a better performance.

- Ratha's method: Ratha et al. (2007) proposed a novel method of template transformation. The general idea is to transform data from original space into another space using one-way function, and the transformed data are stored in the template. They made comparison in the transformation space and used Cartesian coordinates, polar coordinates and kernel function as one-way transfer function. The disadvantage of this method is in the registration phase. Quan et al. (2008) pointed out that the transformation of the form and the parameters proposed by Ratha may restore the original details from the transformation of the template. They proposed three kinds of method to attack transformation template: ARM (attack via record multiplicity) attack, violence attack and compromise equation attack.

This paper focuses on generating secure templates. We directly store and process the original data so that an intruder cannot obtain the permission to extract biometric data even if he/she has the corresponding user's template. Our idea is inspired by the work of Wang et al. (2013), Wu et al. (2016b, c), Chen et al. (2015), Wen et al. (2015), Zheng et al. (2015), Zhu et al. (2016a), Zhu et al. (2016b), Yan et al. (2016) that combines advantages of biometric cryptosystems and feature transformation schemes. The proposed scheme ensures easy revocability. Moreover, our approach is robust toward different images from the same person.

3 Architecture of biometric authentication using secure biometric template

The traditional scheme of secure biometric template is shown in Fig. 1. After feature extraction process, the original biometric template can be abandoned. As long as the transformation template can be stored and transformed, this transformation can be carried out in the signal domain or feature domain. The unreversible transform is under control by some parameters or keys. And under known transform methods, it is very difficult to recover the original features of the information. Therefore, when the stored template is attacked, to achieve the effect of biological characteristics of revocability, we can use a new set of parameters or key control transform function to generate a new template and protect the original biometric information.

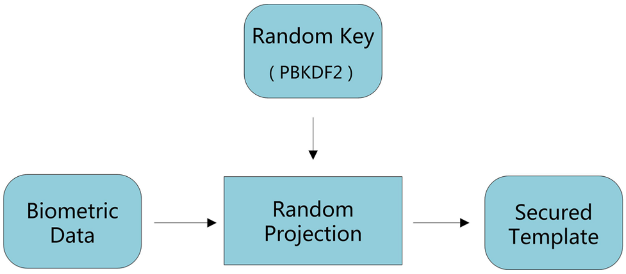


Fig. 2 RP scheme for biometric template

4 Secure biometric template scheme based on deep learning and random projections (FVR-DLRP)

In order to solve above problems and protect the user's information, we proposed a scheme FVR-DLRP for generating secure and renewable template. This scheme uses a random key from user to protect biometric data, shown as Fig. 2.

The overview of proposed scheme is shown in Fig. 3, and the basic components of algorithm FVR-DLRP are shown as below:

- Feature extraction: extract finger vein's endpoints and intersections.

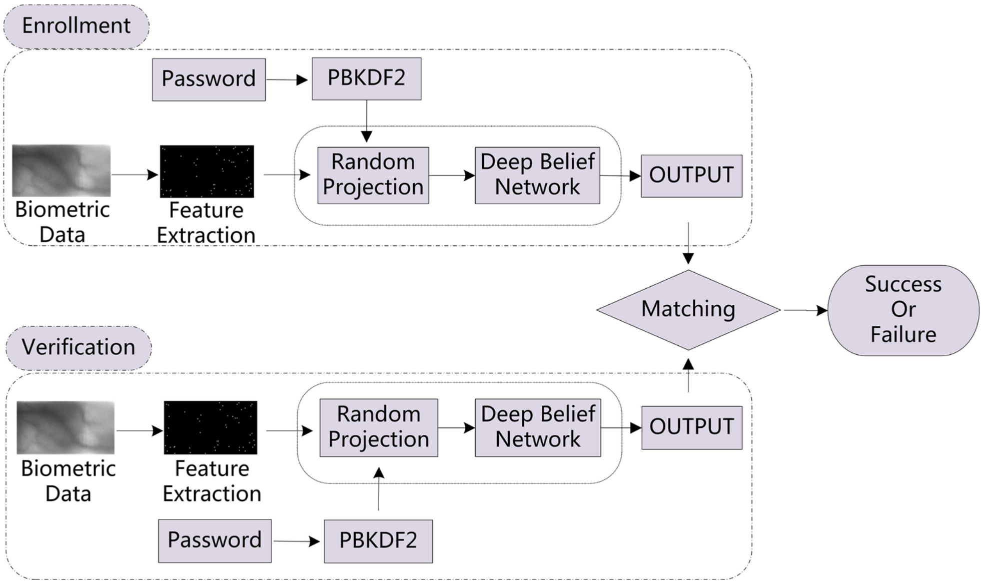
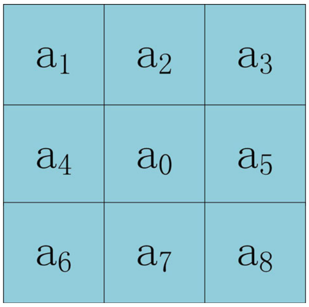


Fig. 3 Architecture of FVR-DLRP scheme



a_1	a_2	a_3
a_4	a_0	a_5
a_6	a_7	a_8

Fig. 4 Feature extraction template

- Random projection: transform high-dimensional data to a lower dimension.
- Training: deep belief networks for training generated template.
- Matching: decision of whether matching the output.

4.1 Finger vein feature extraction

In the pretreatment stage, first we take actions to extract critical information from the image for next processing. Image refinement and feature enhancement are used to reduce noise in finger vein images and improve the contrast ratio between the vein and the background area, meanwhile providing venous information, and extracting feature points set accurately. Image after preprocessing is shown in Fig. 6b. Then we need to extract feature of images. The process is as follows.

We define a 3 × 3 region, as shown in Fig. 4. a_0 is center point, clockwise order around 8 points, successively set to $a_1, a_2, \ldots, a_8$, and the values are 0 or 1.

Fig. 5 Feature points

We define T_N as:

$$T_N = \frac{1}{2} \sum_{i=1}^{8} |a_{i+1} - a_i| \tag{1}$$

When $i = 8$, we define $a_9 = a_1$. If $T_N = 1$, we think a_0 as endpoint; if $T_N \geq 3$, we think a_0 as intersection. The ultimate extracted feature points of finger vein are shown in Fig. 5.

4.2 Random projections for biometric template

Random projection (RP) makes the transformation of high-dimensional data to a relatively low-dimensional space with a rule that distance between points should be set under an satisfied threshold. Assume X is the original data matrix with $m * n$ dimension, R is a random matrix with $k * d$ dimension. To get the output of random project, we need to multiply R and X. Johnson and Lindenstrauss (Quan et al. 2008) have made a great process in the research of random projection. The following Johnson–Lindenstrauss theorem states that it is possible to project n points in a space of arbitrarily high dimension onto an $O(\log n)$-dimensional space. In the reduced dimension, the distance between each pair of points can be approximately retained.

JL theorem. For any $0 < \epsilon < 1$ and any positive integer n, let k be a positive integer such that $k \geq 4(\epsilon^2/2 - \epsilon^3/3)^{-1} \ln n$. Then for any set V of n points in R^d, there is a map $f : R^d \rightarrow R^k$ such that for all $u, v \in V$,

$$(1-\epsilon)||(u-v)||^2 \leq ||f(u)-f(v)||^2 \leq (1+\epsilon)||u-v||^2 \tag{2}$$

In the template protection schemes based on RP, if R is original matrix, we can define transformed templates by $U = RX$ and $V = RY$ and the internal relation is

$$U^T V = X^T Y R R^T = I.$$

But this makes the system vulnerable against attacks. So we need to define a Lipschitz embedding $f(x) = (1/\sqrt{k})Rx$ that satisfied JL theorem, i.e., making the elements of R are independent and identically distributed (IID). Any random matrix's elements chosen from an IID normal distribution $N(0, \sigma^2)$ satisfy JL theorem. We have employed such matric for RP. This can ensure the security of the system for $RR^T \neq I$ and the pair-wise distances are retained. We apply random projections on features of biometric data to reduce the number of feature points. It helps in reduction of computational complexity and makes improvement for DBN process.

The properties of random projections we enumerate are as follows, which will give us a better understanding of the rest of the article. Note that we assume a valid Lipschitz mapping R whose elements are normally distributed with mean $\mu = 0$ and variance σ^2. Here we enumerate six characteristics of R:

1. Vectors in high-dimensional space are orthogonal in any directions, i.e., $RR^T = R^T R$.
2. $E[R^T R] = k\sigma^2 I$ and $E[RR^T] = \mathrm{d}\sigma^2 I$, where R is $k*d$ matrix.
3. Let X^{d*n_1} and Y^{d*n_2} are transformed by R^{k*d} to $U = (\frac{1}{\sqrt{k}\sigma})RX$ and $V = (\frac{1}{\sqrt{k}\sigma})RY$ then

   $$E[U^T V] = X^T Y$$

4. Each element $\epsilon_{i,j}$ of matrix $R^T R$ with $E[\epsilon_{i,j}] = \mathrm{d}\sigma^2$, $Var[\epsilon_{i,j}] = 2\mathrm{d}\sigma^4$.
5. The error $(U^T V - X^T Y)$ generated by random projections and original date has the statistical properties:

   $$E[U^T V - X^T Y] = 0$$
   $$Var[U^T V - X^T Y] = \left(\frac{1}{k}\right)\left(\sigma_i x_i^2 \sigma_i y_i^2 + (\sigma_i x_i y_i)^2\right)$$

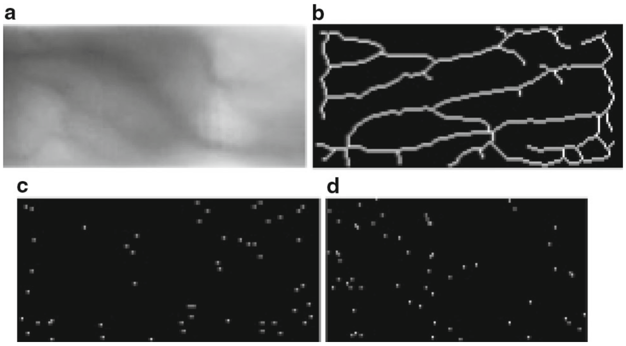


Fig. 6 Original data through random projection. **a** Original data, **b** image after preprocessing, **c** feature extraction of **b**, **d** random projection of **c**

6. When elements of R are chosen from $N(0, 1)$ or from $U(-1, 1)$, then

   $$P(|U^T V - X^T Y| \geq \epsilon) \leq 4 \exp\left(-\frac{k}{4}(\epsilon^2 - \epsilon^3)\right)$$

After operation by random projections R (Fig. 6), we derive from formulas 3–6 based on the statistical independence between observers. In other way, if the data between the observers are lost, the relationship between the features remains (from properties 1 and 2). The biometric template matching algorithm can be directly applied on the U and V, even if the initial biometric data are unknown. It is difficult to conform the specific values of the initial data when the intruder has only the data U or V. This is because there is an infinite number of solutions to the solution of the system's equations. Reduced dimensionality can reduce the error when the projections decrease. Therefore, there is a trade-off between system performance and security level. When the data are sparse, very little information is difficult to reconstruct the raw data. On the other side, if only the random projection is used, the user's biometric information may be leaked.

4.3 Deep belief network for generate biometric template

To make biometric templates more secure, we employ deep belief networks to generate templates.

Now deep belief networks have been widely used in the field of image and speech recognition. Satisfactory recognition results are obtained in the handwriting database. The deep belief network is a multilayer network structure, which can learn the complex mapping relationship between input and output (Hinton et al. 2006). As shown in Fig. 7, there is a deep network model with three hidden layers and one visible layer. The adjacent layers are connected with each other, but the units in the same layer are not connected. The essential part of a DBN is a restricted Boltzmann machine.

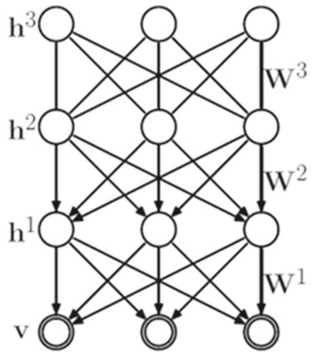


Fig. 7 DBN composed with three RBMs

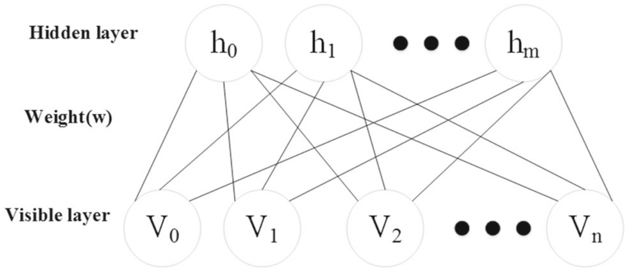


Fig. 8 Restricted Boltzmann machine

- **Restricted Boltzmann machine**

The architecture of RBM is shown in Fig. 8. We can see that it consists of two main layers: one visible layer and one hidden layer. Only the units from different layers are connected.

If visible layer of a RBM has n units and hidden layer has m unites, we can define the energy function of a RBM as:

$$E(v, h; \theta) = -\sum_{i=1}^{n} a_i v_i - \sum_{j=1}^{m} b_j h_j - \sum_{i=1}^{n} \sum_{j=1}^{m} v_i w_{ij} h_j \quad (3)$$

where $\theta = (W, a, b)$ and w_{ij} represents the weights between visible layer and hidden layer; a_i and b_j are their bias. Probability distribution of the DBM is defined as:

$$p(v, h) = \frac{1}{Z} \mathrm{e}^{-E(v,h)} \; Z(\theta) = \textstyle\sum_{v,h} \mathrm{e}^{-E(v,h)}. \quad (4)$$

In general, the probability of visible layer v can be expressed as:

$$p(v) = \frac{1}{Z} \sum_{h} \mathrm{e}^{-E(v,h)} \quad (5)$$

- **Training RBM**

Different from traditional neural network training algorithm, the learning process of the RBM is unsupervised and work as layer by layer. We define $p(v)$ as our likelihood function. However, maximizing the likelihood is not efficient. We employ a contrastive divergence (CD) algorithm, which is a fast learning way for RBM and was introduced by Hinton (2010). We keep updating the weights on the training process until it can satisfy the whole network or complete the set of the number of iteration steps in advance. The Algorithm 1 and Fig. 9 present the details.

Algorithm 1 : Contrastive Divergence, CD

```
Input: RBM($V_1 \dots V_n, H_1 \dots H_m$),training batch $S$
Output: gradient approximation $\Delta w_{ij}, \Delta a_j, \Delta b_i$ for $i = 1, \dots, m, j = 1, \dots, n$
1) Init $\Delta w_{ij} = \Delta a_j = \Delta b_i = 0, for$i = 1, . . . , m, j = 1, . . . , n
2) For all $v \in S$ do
3)     $v^0 \leftarrow v$
4)     For t = 0, . . . , k − 1 do (training period)
5)         For i = 1, . . . , m do sample $h_i^t \sim p(h_i|v^t)$
6)         For j = 1, . . . , n do sample $v_j^{t+1} \sim p(v_j|h^t)$
7)     For i = 1, . . . , m, j = 1, . . . , n do
8)     $\Delta w_{ij} \leftarrow \Delta w_{ij} + p\left(H_i = 1|v^0\right) \cdot v_j^0 - p\left(H_i = 1|v^k\right) \cdot v_j^k$
9)         $\Delta a_j \leftarrow \Delta b_j + v_j^0 - v_j^k$
10)        $\Delta b_i \leftarrow \Delta c_i + p\left(H_i = 1|v^0\right) \cdot v_j^0 - p\left(H_i = 1|v^k\right)$
```

The update rule is defined as:

$$W_{ij}^{\text{new}} = W_{ij}^{\text{old}} + \Delta W_{ij} \quad (6)$$

where $\Delta W_{ij} = \varepsilon((v_i h_j)_{date} - (v_i h_j)_{re})$. Here $(v_i h_j)_{data}$ represents the expectation through training data and $(v_i h_j)_{re}$ represents the expectation through reconstructed data, and ε is the learning data.

- **Training DBN**

We learned the weights of a RBM through a greedy layer-wise unsupervised algorithm. The current trained RBM will

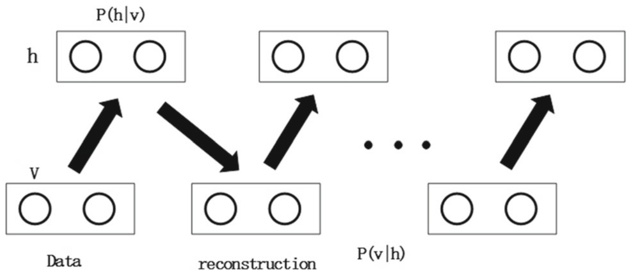


Fig. 9 Training RBM with CD algorithm

take the output of the hidden layer as the input of the next RBM. By this way, which is called pertaining, we can train a whole DBN. This action will make weights between layers fit the whole network more accurately. The unsupervised learning method is the training process of an RBM, which is as follows:

- First initialize all weights to random small values.
- Input the original data by using feature block fusion to the first layer of the whole architecture, and then train the data in the RBM one by one.
- Adjust weights of whole network by using back-propagation algorithm.

4.4 Enrollment phase

During the enrollment phase, users transform the biometric data to a matrix D. Then the endpoints and the intersections of the finger vein will be extracted by a feature extraction model that extracts finger vein's endpoints and intersections. For protecting these features, next they are passed through a secure biometric model. These random projections relay on the value provided by the key, PBKDF2 (Password-Based Key Derivation Function) apply a pseudo random function to derive the key, in a word repeating the hash salted for many times. We take the password as an input of PBKDF2 to generate a key. Data after random projections are used for training deep belief network.

4.5 Verification phase

In verification phase, a series of operations is done during the registration phase. Different biometric information of the same person is preserved. Then these data are performed by feature extract model which outputs the finger vein's endpoints and intersections. Next this feature vector is secured by random projections that take the key produced by the PBKDF2 function as the value and output a secured template.

The matching algorithm DBN performs a comparison between the outputs. For successful authentication, the password provided by user must match the information they store in the template and there must have a great similarity to the secured biometric data.

5 Experiments and performance analysis

To evaluate the efficiency of this algorithm, we use one finger vein laboratory database getting from network named FV_NET64, which contains 64 people's finger vein image, and each of them contributes 15 acquisitions. Thus, this database contains 960 pictures, whose dimensions are all 70*150. In the simulation experiment, we choose 12 figures of each one for the net training, and the remainders are for testing. Our DBN model consists of two RBMs, the input layer needs 10,500 nodes, then the first RBM layer has 1000 nodes, and the second RBM layer exists 100 nodes. The network structure is 10,500–1000–100. The initial weights bias of different layer is set to 0. Two RBMs are enough for us in this system, because we only have 10 pictures to feed the whole network as one batch, too deep structure can not get fully trained. The false acceptance rate (FAR) and recognition rate (GAR) are employed to evaluate our proposed scheme.

The result of our experiments is shown in Table 1. We use different values of k to observe whether the compression degree would effect the authentication. We note that deeper compress, the worse performance will be obtained. Furthermore, we compare different methods with our proposed method, such as Hausdorff distance (HD) schemes proposed by Li et al. (2007) and principal component analysis (PCA) proposed by Wang (2007) on finger vein recognition. Table 2 displays the different results of some traditional algorithms. We can see that the DBN algorithm can achieve better results.

Table 3 reports the verification performance of the system before and after transformation. As we can see, there is little

Table 1 Authentication performance of different value k

k	GAR (%)	FAR (%)
5	96.9	1.5
10	94.3	1.2
15	93.5	0.8
20	91.8	0.3

Table 2 Authentication performance of different approaches

Method	GAR (%)	FAR (%)
DBN	96.9	1.5
Hausdorff distance (HD)	92.4	5.2
PCA	95	4.3

Table 3 Authentication performance before and after FVR-DLRP

k	GAR (%)		FAR (%)	
	Before	After	Before	After
5	96.9	95.3	1.5	2.2
10	94.3	94	1.2	1.2
15	93.5	92.2	0.8	1.3
20	91.8	91.2	0.3	0.3

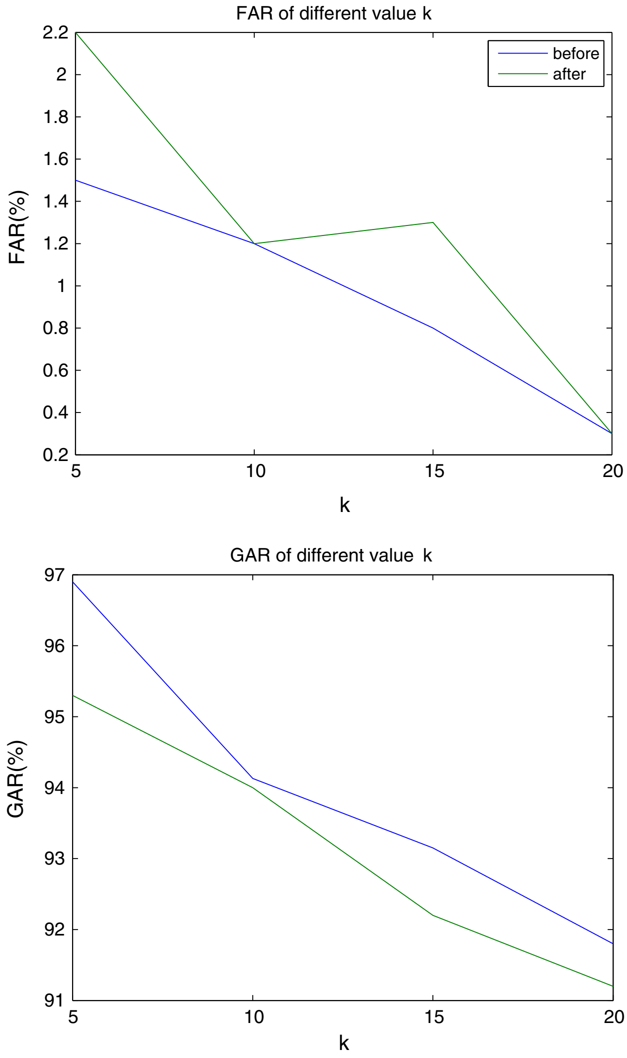


Fig. 10 Authentication performance before and after FVR-DLRP

change before and after transformation, so we can prove the correctness of the theoretical analysis. As shown in Fig. 10, we can observe more intuitive on verification performance with different value of *k* before and after transformation.

6 Conclusions

This paper presents a secure and efficient framework to generate secure, efficient and revocable biometric templates. The new framework employs deep belief networks and random projections of biometric data using secure keys from passwords for user verification. The biggest bright spot of the proposed system is that it can keep the most important information of biometric data, even the password is decoded. And this is the kernel part of feature transformation techniques. We try some methods to display the performance of proposed system, and the result shows that random transformation can enhance the revocability of the template and the dynamic mapping can enhance the uncertainty of the transformation. We argue that there is no perfect template protection technology which can meet the requirements of all biological characteristics and applications. In addition, test environment will change in training and recognition process, resulting in the deviation of dynamic mapping matrix. In the future research, we will focus on proposing constructions fitting complicated conditions and exploring other recognition algorithms with ability of template protection.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61572144), the Natural Science Foundation of Guangdong (2014A030313517), the Science and Technology Planning Project of Guangdong Province (2015B010129015, 2013B040500009), the Zhejiang Sicence Fund No. LY16F020016 and the Innovation Team Project of Guangdong Universities (No 2015KCXTD014).

Compliance with ethical standards

Conflict of interest Yi Liu, Jie Lin, Zhusong Liu, Jian Shen and Chongzhi Gao all declare that they have no conflict of interest.

References

Ang R, Safavi-Naini R, Mcaven L (2005) Cancelable key-based fingerprint templates. In: Proceedings of the Australasian conference information security and privacy (ACISP 2005), Brisbane, Australia, July 4–6, 2005, pp 242–252

Chen C, Wu Z, Li P, Zhang J, Wang Y, Li H (2015) A finger vein recognition algorithm using feature block fusion and depth neural network. In: International symposium on intelligence computation and applications, Springer, Berlin, pp 572–583

Gu B, Sheng VS, Tay KY, Romano W, Li S (2014) Incremental support vector learning for ordinal regression. IEEE Trans Neural Netw Learn Syst 26(7):1403–1416

Hinton GE (2010) A practical guide to training restricted Boltzmann machines. Momentum 9(1):599–619

Hinton GE, Osindero S, Teh YW (2006) A fast learning algorithm for deep belief nets. Neural Comput 18(7):1527–1554

Jain AK, Ross A, Uludag U (2005) Biometric template security: Challenges and solutions. In: 2005 13th European signal processing conference. IEEE, pp 1–4

Kong A, Zhang D, Kamel M (2008) Three measures for secure palmprint identification. Pattern Recogn 41(4):1329–1337

Li X, Guo S, Gao F, Li Y (2007) Vein pattern recognitions by moment invariants. In: The international conference on bioinformatics and biomedical engineering, pp 612–615

Li J, Chen X, Li M, Li J, Lee PPC, Lou W (2013) Secure deduplication with efficient and reliable convergent key management. IEEE Trans Parallel Distrib Syst 25(6):1615–1625

Li J, Li X, Yang B, Sun X (2015a) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur 10(3):507–518

Li J, Li YK, Chen X, Lee P, Lou W (2015b) A hybrid cloud approach for secure authorized deduplication. IEEE Trans Parallel Distrib Syst 26(5):1206–1216

Lim MH, Teoh ABJ, Toh KA (2012) An efficient dynamic reliability-dependent bit allocation for biometric discretization. Pattern Recognit 45(5):1960–1971

Liu Z, Yin Y, Wang H, Song S, Li Q (2010) Finger vein recognition with manifold learning. J Netw Comput Appl 33(3):275–282

Maio D, Nanni L (2005) Multihashing, human authentication featuring biometrics data and tokenized random number: a case study fvc2004. Neurocomputing 69(1):242–249

Maiorana E (2010) Biometric cryptosystem using function based online signature recognition. Expert Syst Appl 37(4):3454–3461

Nanni L, Lumini A (2008) Random subspace for an improved biohashing for face authentication. Pattern Recognit Lett 29(3):295–300

Pankanti S, Jain A, Hong L (2000) Biometrics: promising frontiers for emerging identification market. Comm ACM 43:91–98

Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of ratha. In: International symposium on computer science and computational technology, pp 572–575

Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634

Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572

Rua EA, Maiorana E, Castro JLA, Campisi P (2012) Biometric template protection using universal background models: an application to online signature. IEEE Trans Inf Forensics Secur 7(1):269–282

Shen J, Tan H, Wang J, Wang J, Lee S (2015) A novel routing protocol providing good transmission reliability in underwater sensor networks. J Internet Technol 16(1):171–178

Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–960

Wang KJ (2007) Finger vein recognition based on wavelet moment fused with PCA transform. Pattern Recognit Artif Intell 20(5):692–697

Wang J, Ma H, Tang Q, Li J, Zhu H, Ma S, Chen X (2013) Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. Comput Sci Inf Syst 10(2):667–684

Wen X, Shao L, Xue Y, Fang W (2015) A rapid learning algorithm for vehicle classification. Inf Sci 295:395–406

Wu Z, Liang B, You L, Jian Z, Li J (2016a) High-dimension space projection-based biometric encryption for fingerprint with fuzzy minutia. Soft Comput 20(12):4907–4918

Wu Z, Yu Z, Yuan J, Zhang J (2016b) A twice face recognition algorithm. Soft Comput 20(3):1007–1019

Wu Z, Yuan J, Zhang J, Huang H (2016c) A hierarchical face recognition algorithm based on humanoid nonlinear least-squares computation. J Ambient Intell Human Comput 7(2):229–238

Yan F, Tan Y, Zhang Q, Wu F, Cheng Z, Zheng J (2016) An effective raid data layout for object-based de-duplication backup system. Chin J Electron 25(5):832–840

Zheng Y, Byeungwoo J, Xu D, Wu QMJ, Zhang H (2015) Image segmentation by generalized hierarchical fuzzy c-means algorithm. J Intell Fuzzy Syst 28(2):4024–4028

Zhu R, Ya Tan, Zhang Q, Fei W, Zheng J, Yuan X (2016a) Determining image base of firmware files for arm devices. IEICE Trans Inf Syst 99(2):351–359

Zhu R, Ya Tan, Zhang Q, Li Y, Zheng J (2016b) Determining image base of firmware for arm devices by matching literal pools. Dig Investig 16:19–28