Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

A Secure Finger Vein Recognition Algorithm Based on MB-GLBP and Logistic Mapping

Lin You, Jiawan Wang, Bin Yan
School of Communication Engineering
Hangzhou Dianzi University, Hangzhou 310018, China
mryoulin@gmail.com, holyjw@163.com, yanbin0061@gmail.com

Received November, 2015; revised June, 2016

Abstract. *A secure finger vein recognition algorithm based on MB-GLBP and Logistic Mapping is developed. The algorithm includes three stages. Firstly, the MB-GLBP (Multi-scale Block Gabor Local Binary Patterns) algorithm is performed on the finger vein images which have been normalized to extract the initial features. Secondly, the Logistic Mapping is employed to scramble and encrypt those feature data. Finally, the matching is accomplished by computing the Euclidean distances among the final feature templates of the training samples and the testing samples. Our experimental results indicate that our new method has good recognition effect and high security.*

Keywords: MB-GLBP, Gabor, LBP, Logistic Mapping, Finger vein, Template protection

1. Introduction.

Finger vein recognition technology is a new biometric recognition technology, which accomplishes the matching step by comparing the feature templates extracted from finger vein images with the feature templates registered before. With good specificity and high security, it has become a hot research topic in biometric recognition and a lot of theoretical work and applications have been done[1, 3, 4, 10, 11]. And the verification rate and security are important criterions to determine the performance of finger vein recognition algorithm.

LBP (Local Binary Patterns) is defined as a gray-scale invariant texture description operator, which is proposed and applied to the pattern recognition by Harwood et al [2]. In 2012, Wang et al [3] applied the LBP algorithm to the finger vein recognition successfully, but the verification rate of their algorithm was not so ideal. In order to improve the verification rate of the finger vein recognition algorithm based on LBP, Peng et al [4] proposed a new finger vein recognition algorithm based on GLBP (Gabor Local Binary Patterns) in 2013. The essence of their algorithm is combining the Gabor filter with the LBP algorithm. Firstly, it got the finger vein images of multi-scales and multi-orientations using the Gabor filter to decompose the original image. Then it extracted the vein features of these images by the LBP algorithm. Finally, it accomplished the matching by comparing the gotten LBP feature templates with the registered LBP feature templates. In order to improve the verification rate of the finger vein recognition algorithm further, we propose a finger vein recognition algorithm based on MB-GLBP for identity verification, which combines the Gabor filter with the MB-LBP algorithm.

However, with the development of information technology, it is not enough to just obtain good verification rate for the finger vein recognition algorithm, because the security of the feature templates must be guaranteed at the same time. Therefore, many biometric template protection algorithms have been proposed, such as the fuzzy vault described in [5] and the Biohash algorithm described in [6]. Whereas, what they concerned are fingerprint features and facial features instead of finger vein features.

In order to improve the security of the finger vein recognition, we propose a secure finger vein recognition algorithm based on MB-GLBP and Logistic mapping. Firstly, we extract the finger vein features by the MB-GLBP algorithm. Then we scramble and encrypt those features with the Logistic mapping generated by the user's password. Finally, we accomplish the matching step by computing the Euclidean distance among the final feature templates of the training samples and the testing samples. Our experimental results indicate that our algorithm has good verification rate and high security.

2. A Secure Finger Vein Recognition Algorithm Based on MB-GLBP and Logistic Mapping.

The finger vein templates generated by the traditional finger vein recognition algorithms are unique and irrevocable. Once their finger vein templates are stolen, the users have to adopt other fingers to register. It not only can bring troubles to the users, but also may cause problems such as irreparable damages to property and so on. In order to protect the finger vein templates' security and the users' privacy, we propose a secure finger vein recognition algorithm combined the MB-GLBP algorithm with the Logistic mapping, and the algorithm flow chart is shown in Figure 1.

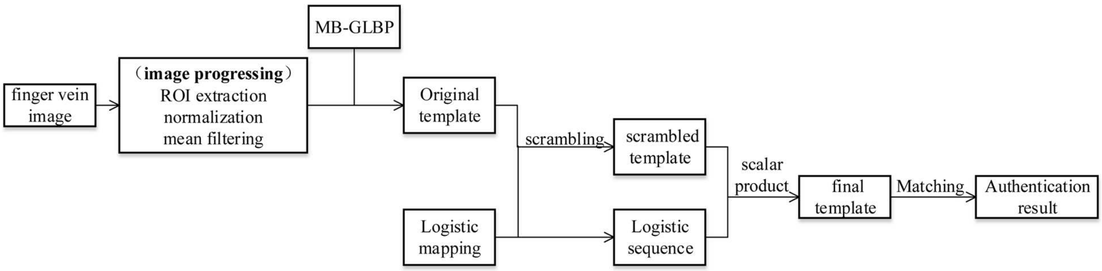


Figure 1. Flowchart of our algorithm.

2.1. Image Progressing.

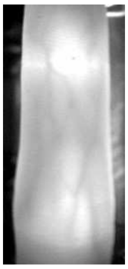
It is inevitable that there are many external factors which disturb the vein image acquisition process, such as illumination changes and finger's displacement changes. And those factors will make the vein images contain a lot of noise. In order to reduce the influence of noise and speed up the training rate of our algorithm, we employ size scale and gray scale normalization to the original vein image, which converts the original vein image of size 300 × 140 into the clearer vein image of size 150 × 70. After that, the image will be filtered with the mean filter, which can remove some noise interferences, as shown in Figure 2.

2.2. MB-GLBP Algorithm.

In order to reduce the influence of noise further and improve the verification rate of our algorithm, we propose a finger vein algorithm based on MB-GLBP combining the Gabor kernel function with the MB-LBP algorithm. It contains two parts as follows:

(1) Gabor kernel function

The trajectory of Gabor kernel function is similar to the stimulate response curve of human visual cells, and it has good properties in terms of extracting target's local



(a) original image (b) preprocessed image

Figure 2. Image progressing.

spatial information frequency domain information. In addition, taking the LBP operator on the Gabor amplitude images can extract relevant frequency domain characteristics with different numbers of the size scale and the orientation from the Gabor images effectively [7].Therefore, we can filter and decompose the original vein images by a set of Gabor filters with different numbers of the size scale and the orientation to mitigate the influences of illumination and displacement on the verification rate.

We use the following forms of Gabor kernel function:

$$g_{\mu,v}(x,y) = \frac{\parallel K_{\mu,v} \parallel^2}{\sigma^2} e^{-\frac{\|K_{\mu,v}\|^2(x^2+y^2)}{2\sigma^2}} \left[e^{iK_{\mu,v}\cdot \begin{pmatrix} x \\ y \end{pmatrix}} - e^{-\frac{\sigma^2}{2}} \right] \quad (1)$$

where $K_{\mu,v} = \begin{pmatrix} K_v cos\phi_\mu \\ K_v sin\phi_\mu \end{pmatrix}$, $K_v = 2^{-\frac{v+2}{2}}$, $\phi_\mu = \frac{\pi\mu}{8}$, μ and v are the numbers of the orientation and the size scale of the Gabor kernel function respectively, σ is the variance of Gabor filter images.

The Gabor feature images can be gotten by convolving original vein image with the Gabor kernel function. When we set the Gabor filter as four orientations $\mu \in \{0,1,2,3\}$ and three size scales $v \in \{0,1,2\}$, we can get 12 features, as shown in Figure 3.

(2) MB-LBP algorithm

In order to get the local spatial changing information of the sampled Gabor feature images, we extract the Gabor feature images by the MB-LBP algorithm further.

MB-LBP algorithm is the improved algorithm of the traditional LBP algorithm. And the traditional LBP algorithm often extracts features with a rectangle block of size 3 × 3. That is, it takes the center pixel p_c of the rectangular block as the reference point to carry out binarization processing on the 8 pixels $p_i (i = 0, 1, ..., 7)$ around, and if its pixel value is greater than p_c, it assigns its value to 1, or assigns its value to 0. Finally, we compute its LBP value as Eq. 2:

$$LBP = \sum_{i=0}^{7} S(p_i - p_c)2^i, (i = 0, 1, ..., 7) \quad (2)$$

where $S(x) = \begin{cases} 1 & x > 0 \\ 0 & x < 0 \end{cases}$.

Figure 4 is the diagram of the traditional LBP algorithm.

The traditional LBP algorithm has the advantages of rotation invariance and grayscale invariance, but it only considers the gray level difference among pixels

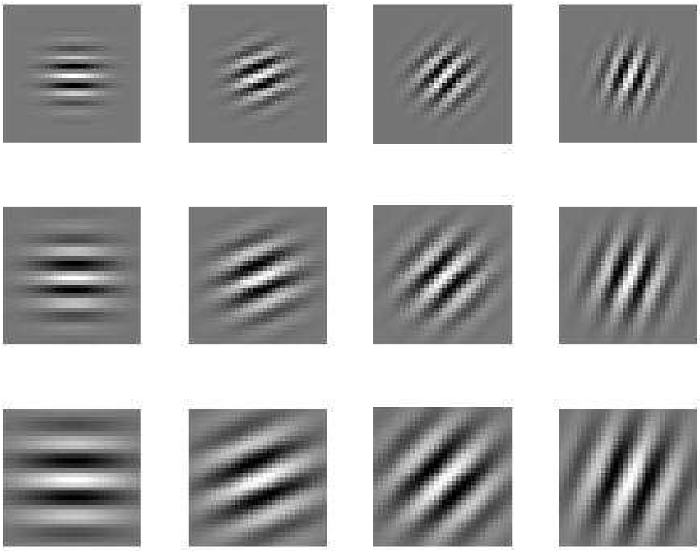
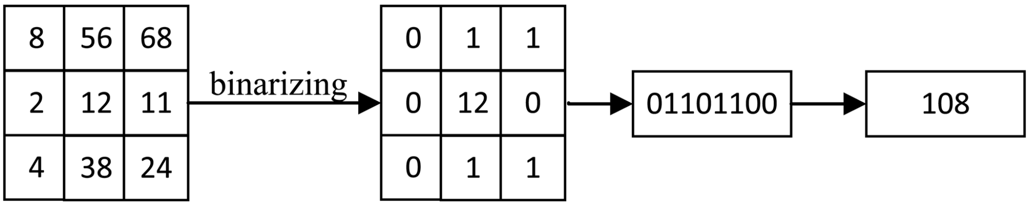


Figure 3. The Gabor feature images.

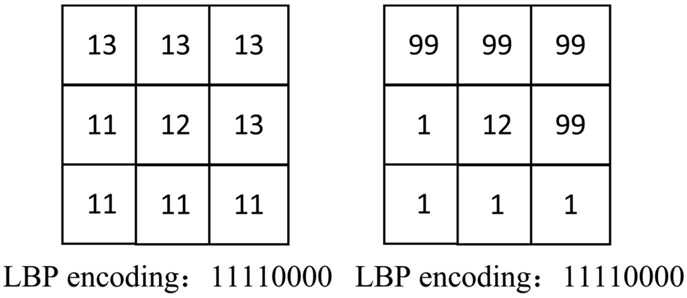


8	56	68
2	12	11
4	38	24

0	1	1
0	12	0
0	1	1

Figure 4. The diagram of the LBP algorithm.

while ignores the contrast among pixels. Therefore, when the contrast among pixels changes greatly by strong illumination change, some important texture description features will be easily lost, as shown in Figure 5.



13	13	13
11	12	13
11	11	11

99	99	99
1	12	99
1	1	1

LBP encoding：11110000 LBP encoding：11110000

Figure 5. The grayscale values of the local areas is different but its LBP code is the same.

In order to change this situation, the grayscale values of the local areas is different but its LBP code is the same, Garish et al [8] propose the MB-LBP algorithm, which got the new LBP encoding by comparing values of the pixels around with the subdomain average gray value instead of the gray value of the center pixel. Figure 6 shows the diagram of the MB-LBP algorithm.

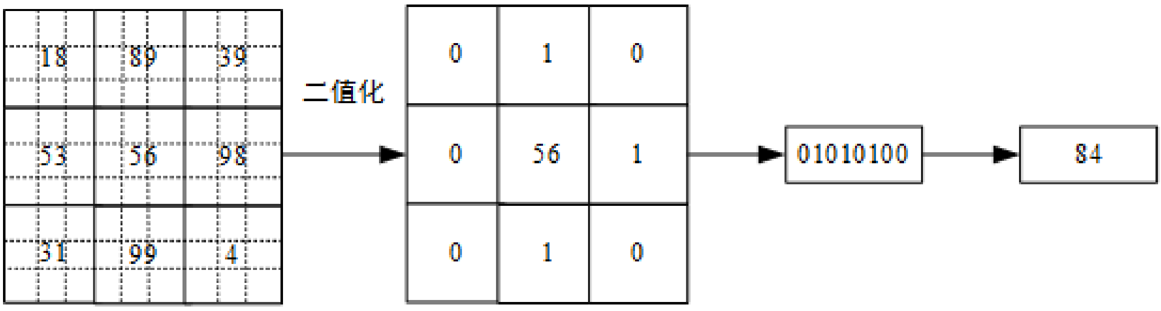


FIGURE 6. The diagram of the MB-LBP algorithm.

The MB-GLBP algorithm include three steps. Firstly, the features of the original finger vein images from multi-scales and multi-orientations is extracted by the Gabor kernel function to get N Gabor feature images. After that, the feature vectors of those images is computed using the MB-LBP algorithm and histogram statistics. At last, it those N eigenvectors is cascaded to store as the feature template of the vein image for encrypting further.

2.3. **Logistic Mapping.**

Logistic mapping is a classic model of chaotic mapping. It is defined as follows:

$$x_{k+1} = \mu x_k(1 - x_k) \tag{3}$$

where $0 \leq \mu \leq 4$, $x_k \in (0, 1)$, $k \in \{0, 1, 2, 3, 4, ...\}$. According to [9], the Logistic mapping will be in a chaos state if $3.5699456 < \mu < 4$. At the moment, the sequence generated by Logistic mapping is aperiodic, divergent and sensitive to the initial value. Additionally, it has good randomness and ergodicity, and distributes equally- probabilistically on the domain. Thus, it is very suitable for image encryption. Figure 7 is its bifurcation diagram.

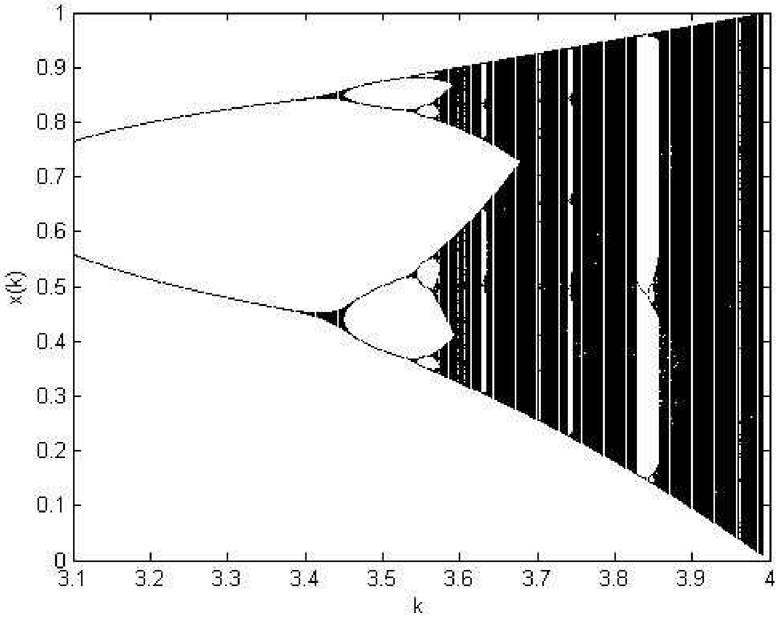


FIGURE 7. Logistic mapping bifurcation diagram.

2.4. **Feature Encryption.**

Suppose that, after taking the MB-GLBP algorithm on the original image, we get N feature vectors, that is, the original feature template. In order to protect the template, we scramble and encrypt it with the Logistic mapping. The concrete encryption steps are as follows:

(1) Set the original feature template as $M_0 = [\alpha_1, \alpha_2, ..., \alpha_N]$, where $\alpha_i = [a_{i_1}, a_{i_2}, ..., a_{i_n}]^T$, N is the number of the feature vectors, n is the length of the feature vectors.

(2) Generate a user password m with fixed length randomly and divide it into two parts m_1 and m_2.

(3) Convert m_1 and m_2 to be the initial values of the chaotic systems S_1 and S_2 using a random floating-point numbers generator, respectively.

(4) Generate a chaotic real number sequence of a fix-length N with the chaotic system S_1, and denote it as $M_1 = [\beta_1, \beta_2, ..., \beta_N]$, where $\beta_i = [b_{i_1}, b_{i_2}, ..., b_{i_n}]^T$.

(5) Take an ascending order on β_i to get the sequence $\beta_i' = [b_{i'_1}, b_{i'_2}, ..., b_{i'_n}]$, and record the subscripts of the sequence β_i' as $p_i = [i'_1, i'_2, ..., i'_n]^T$;

(6) Rearrange the sequence α_i according to the p_i to get the sequence $\alpha_i' = [a_{i'_1}, a_{i'_2}, ..., a_{i'_n}]^T$ after being scrambled, and then get the scrambled sequence $M_2 = [\alpha_1', \alpha_2', ..., \alpha_N']$, that is, the scrambled feature template;

(7) Generate a chaotic real number sequence of a fix-length N with the chaotic system S_2, and denote it as $M_3 = [\gamma_1, \gamma_2, ..., \gamma_N]$, where $\gamma_i = [r_{i_1}, r_{i_2}, ..., r_{i_n}]^T$, and then convert M_3 to a random binary sequence $M_4 = [\eta_1, \eta_2, ..., \eta_N]$;

(8) Take a scalar product on the elements in M_4 and M_2, and let the product be M, that is, $M = [\alpha_1' \cdot \eta_1, \alpha_2' \cdot \eta_2, ..., \alpha_N' \cdot \eta_N]$, and then get the final feature template.

3. **Experimental Results and Analysis of Security.**

3.1. **The Experimental Database.**

To verify the validity of our algorithm, our laboratory have established a finger vein image database. It is composed of the finger vein images captured from 70 different fingers, and each finger has eight images collected in different time, which have illuminations and position changes from each other. That is, there are 560 images in all. Figure 8 is four different images from the same finger. Figure 9 is four different images from the four different fingers.

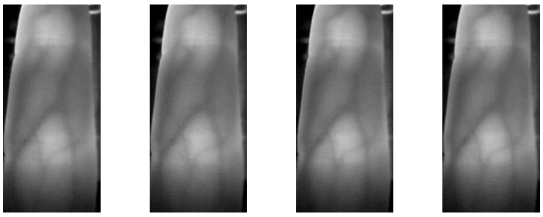


FIGURE 8. Four different images from the same finger.

3.2. **Parameter Selection of The Gabor Kernel Function.**

In order to enhance the recognition effect of the MB-GLBP algorithm as much as possible, we must take an optimal combination of the numbers of the size scale and orientation in the Gabor kernel function. Although there are myriad numbers of the orientation in the Gabor kernel function, the total time of feature extracting and matching will be too long with excessive numbers of the orientation, and the verification rate will tend towards stable when the number of the orientation increases to a certain extent.

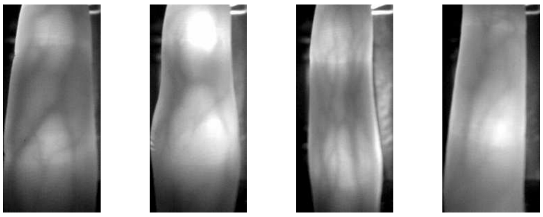


FIGURE 9. Four different images from the four different fingers.

Thus, we choose the number of the orientation in the Gabor kernel function as $i \in \{1, 2, ..., 16\}$, that is, when the number of the orientation is i , the values of the orientation are $\pi/i, \pi * 2/i, ..., \pi * (i-1)/i$. In addition, due to the restrictions of the vein image size (the size of the normalized finger vein images is 70×150), we choose the number of the size scale as $j \in \{1, 2, 3, 4, 5\}$ for our experiment, and compute the verification rate by the nearest neighbor classification and the Euclidean distance.

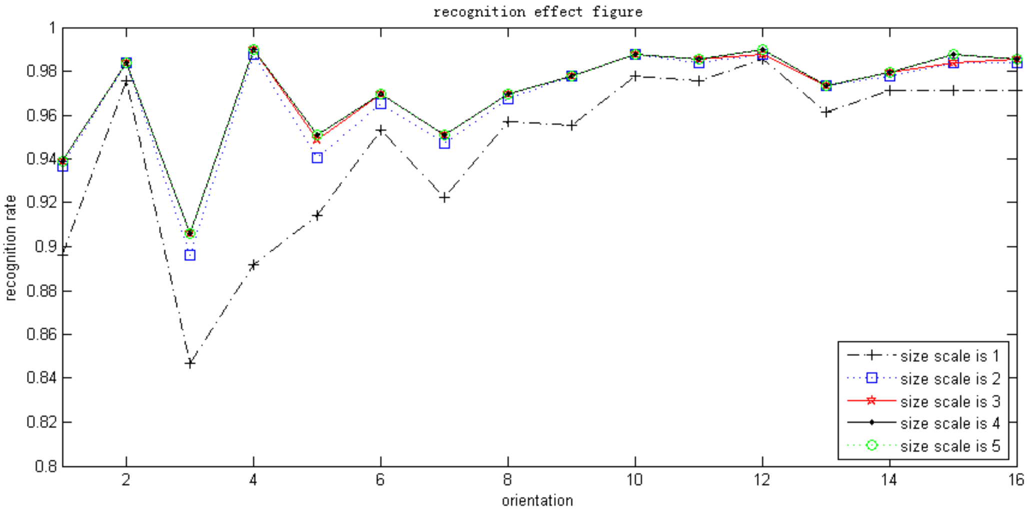


FIGURE 10. Recognition effect figure in different numbers of the size scale and the orientation.

Figure 10 is the recognition effect figure in different numbers of the size scale and the orientation. From this figure, we can see that when the number of the size scale remains constant, the verification rate of our algorithm will tend to be stable with the increasing of the orientation number. In addition, the recognition effect is better when the number of the size scale is 3 rather than 1 or 2, and the verification rate is almost the same when the number of the size scale is 3, 4 or 5. At last, when the combination of the numbers of the size scale and the orientation in the Gabor kernel function is 3×4, 4×4, 4×12 or 5×12, the verification rate of our algorithm achieves the maximum value 0.9898.

In order to take an optimal combination of the numbers of the size scale and the orientation in the Gabor kernel function further, we test the recognition time when the numbers of the size scale and the orientation are different. From Table 1, we can see that when the number of the size scale remains constant, the recognition time will increasing with the number of the orientation increasing; From Table 2, we can see that when the number of the orientation remains constant, the recognition time will increasing with the number of the size scale increasing.

Table 1. Recognition time contrast when the number of the orientations is different(size scale is 3).

Orientation	Total time for feature extraction	Total time for matching	Total time
1	19.8251	0.6143	21.4394
2	24.6157	0.9568	27.5725
3	29.2979	1.4797	33.7776
4	34.1279	1.7609	39.8888
5	39.7050	1.8836	46.5886
6	43.1769	2.6589	51.8358
7	52.5018	2.8904	62.3922
8	57.7573	3.3426	69.0999
9	67.7513	3.7241	80.4754
10	71.9572	4.1126	86.0698
11	84.8722	4.4957	100.3679
12	95.6293	4.7224	112.3517

Table 2. Recognition time contrast when the number of the size scales is different(orientation is 4).

Size scale	Total time for feature extraction	Total time for matching	Total time
1	31.3292	0.7472	33.0764
2	33.1215	1.3605	36.4820
3	34.1279	1.7609	38.8888
4	36.6414	1.8510	42.4924
5	39.3004	2.1008	46.4012

In conclusion, in order to improve the verification rate and reduce the recognition time as much as possible, we should set the combination of the numbers of the size scale and the orientation as 3 × 4, whose verification rate reaches 0.9898.

3.3. **Parameter Selection of Logistic Mapping.**

(1) Verification Rate Comparison under Different Initial Values

In order to prove that the Logistic sequence produced by Logistic mapping can be used to encrypt the vein feature data, we compare the first 100 sequences produced by the Logistic mapping when the initial values are 6.0000 and 6.0001 respectively, the Logistic mapping is surjective ($\mu = 4$) and its iterations is 64, as shown in Figure 11.

We can see from Figure 11 that the Logistic sequence distributions are very different, although the difference of their initial values is only 10^{-4}.

In order to prove that the Logistic sequence can be used to encrypt the vein feature data further, we extract any 100 feature data from the vein feature vectors generated by the MB-GLBP algorithm, and scramble and encrypt them with the sequence shown in Figure 11, as shown in Figure 12 and 13. From those figures, we can see that the data scrambled and encrypted are different when their initial values are different.

(2) Verification Rate Comparison under Different Bifurcation Parameters

In order to analyze whether the encryption result is associated with the bifurcation parameters of the Logistic mapping and study the impacts of scrambling

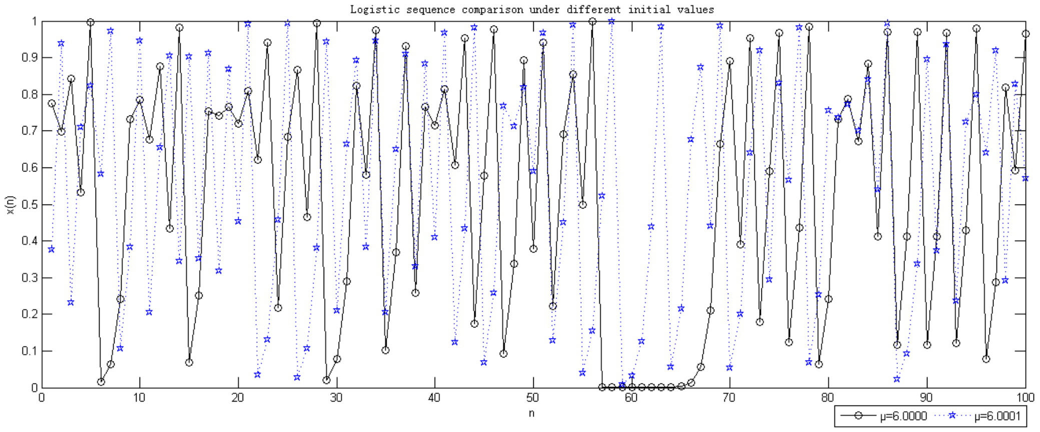


Figure 11. Logistic sequence comparison under different initial values.

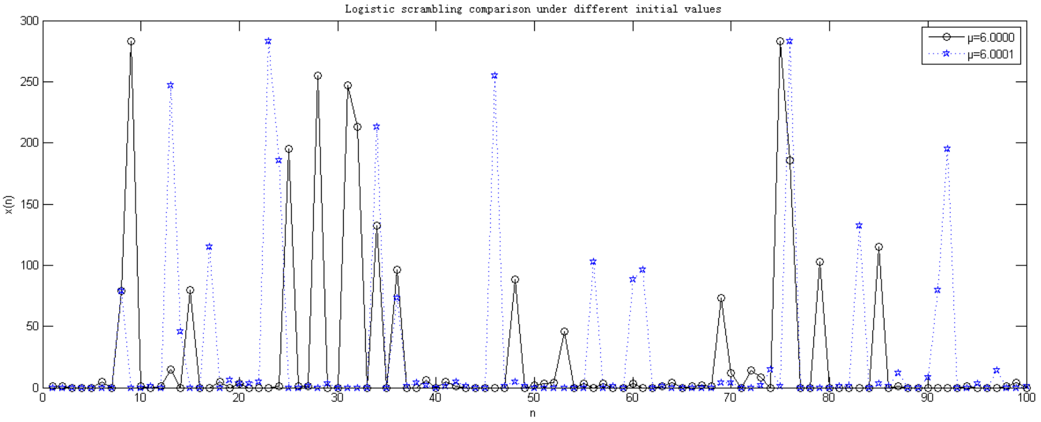


Figure 12. Logistic scrambling comparison under different initial values.

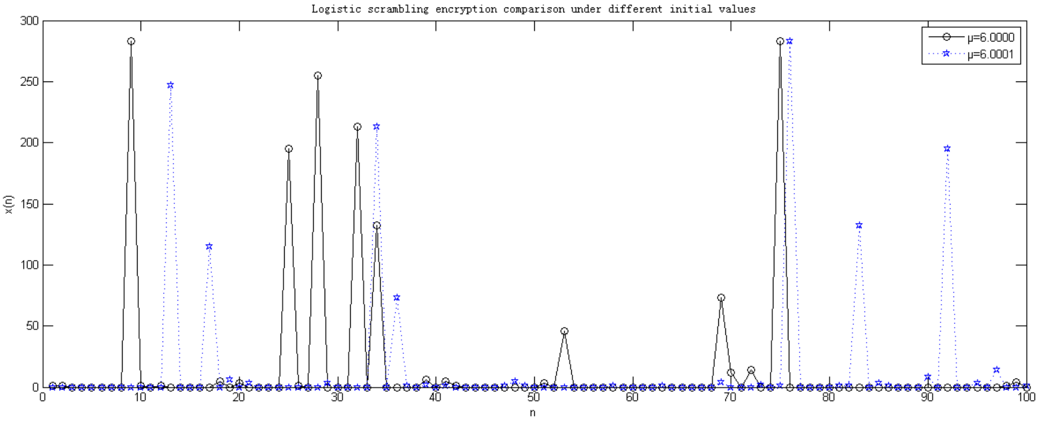


Figure 13. Logistic scrambling encryption comparison under different initial values.

encryption on the MB-GLBP algorithm's verification rate, we set the initial value of the Logistic mapping as 0.6, and choose the bifurcation parameters μ as 3.6, 3.7, 3.8, 3.9 or 4.0 controlling the Logistic mapping in a state of chaos. And then we scramble and encrypt the feature vectors generated by the MB-GLBP algorithm with the Logistic sequences whose bifurcation parameters is 3.6, 3.7, 3.8, 3.9 or 4.0. After that, we choose the threshold value by computing the Euclidean distances of the feature templates in the illegal and legal matchings respectively. Finally, we can get the verification rate (VR), equal error rate (EER), FAR and the ROC curve.

Table 3 is the comparison of the verification rate between the MB-GLBP algorithm and our algorithm encrypted by the Logistic mapping with different μ, and Figure 14 is their ROC curve. From them, we can see that scrambling and encrypting the feature vectors using the Logistic mapping has no big impact on the verification rate of the MB-GLBP algorithm. Meanwhile, for one thing, when the value of FAR is constant, the verification rate of our encryption algorithm which $\mu = 3.6$ is the most close to that of the unencrypted MB-GLBP algorithm; for the other thing, when the value of FAR is less than or equal to 1%, the recognition rate of our encryption algorithm with $\mu = 3.6$ is the highest, and the smaller the value of FAR, the better the effect of recognition. And so, when $\mu = 3.6$, the recognition of our algorithm is the best.

In addition, we measure that the EER of the MB-GLBP algorithm is 1.9%, and when the μ is 3.6, 3.7, 3.8, 3.9 or 4.0, the EER of our algorithm is 1.9%, 2.1%, 2.1%, 2.7%, 2.1% or 3.1% respectively. Thus, we can see that Logistic scrambling and encryption has no big impact on the EER of the MB-GLBP algorithm, and when $\mu = 3.6$, the recognition of our algorithm is the best.

In conclusion, our encryption algorithm can not only scramble and encrypt the vein feature data effectively, but also can protect the data while maintaining good recognition effect.

Table 3. FAR and verification rate comparison for different μ.

FAR(%)	unencrypted	$\mu = 3.6$	3.7	3.8	3.9	4.0
0.01	0.6907	0.5598	0.5978	0.4979	0.4979	0.4802
0.1	0.8777	0.8232	0.8301	0.7393	0.7804	0.7388
1	0.9712	0.9621	0.9567	0.9220	0.9220	0.9172
10	0.9947	0.9952	0.9915	0.9915	0.9931	0.9957
20	0.9989	0.9979	0.9968	0.9968	0.9984	0.9984

3.4. Security Analysis on Our Algorithm.

As the traditional finger vein recognition algorithms have not taken any encryption operations on the finger vein feature data, it will be cracked easily and cause an great threat for users' privacy security and property security.

Our algorithm takes the double factor authenticates, vein features extraction and password encryption. We split a random password into two parts which are randomly mapped into the initial values of the Logistic mapping, and then use them to generate a Logistic sequence of real numbers and a Logistic binary sequence. At last, using the former to scramble the feature vectors and the latter to encrypt it, we get the final feature data. Therefore, if a hacker want to invade our vein recognition system, he must crack the user's password and get the vein image at the same time, and it is obviously impossible. When a hacker has gotten the user's encrypted feature data and wants to restore the original

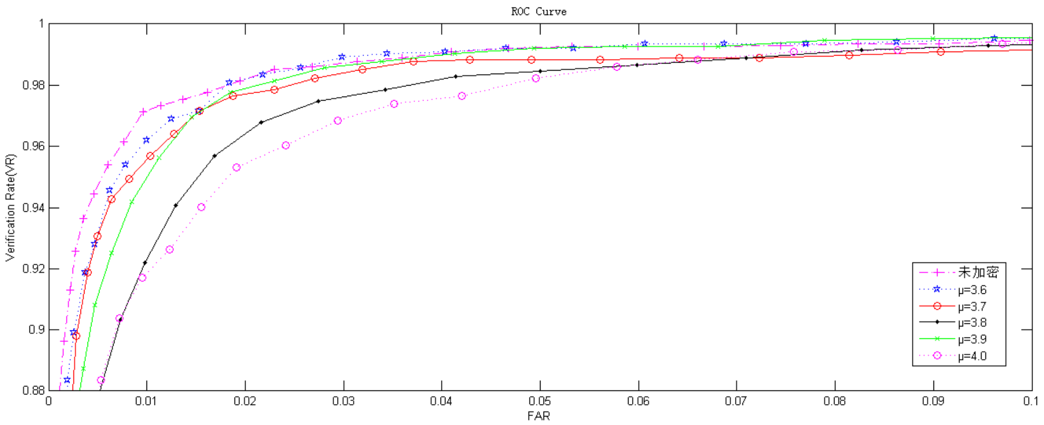


Figure 14. ROC curve under different μ.

vein feature, he must crack the user's password. In addition, the feature information our algorithm extracted and encrypted by the Logistic sequence is only a part of the vein feature vectors, and our algorithm is unidirectional, so it is almost impossible to restore user's original vein feature data. What's more, when a user knows his vein data leaked, he can also identify himself again by changing his password or using other fingers to register. In conclusion, our algorithm is safer than the traditional finger vein algorithm, and it can protect the original vein data effectively.

3.5. Comparisons of Some improved Algorithms Based on LBP.

In order to verify the effectiveness of our algorithm further, we compare the EER and the security of our algorithm and other improved finger vein recognition algorithms based on LBP, and the results are shown as the table below:

Table 4. comparisons of some improved algorithms based on LBP.

Algorithms	EER(%)	security
LBP	1.8	no encryption, and no operation to enhance algorithm's security
PBBM(Personalized Best Bit Map) [10]	3.2	no encryption, and no operation to enhance algorithm's security
PDBM(Personalized Discriminative Bit Map) [11]	3.2	no encryption, and no operation to enhance algorithm's security
MB-GLBP	1.9	no encryption, but have operation to enhance algorithm's security
our algorithm	1.9	encryption, and have operation to enhance algorithm's security

From table 4, we can see that the ERR of our algorithm is lower than that of the traditional finger vein recognition algorithm based on LBP, and is equal to the improved finger vein recognition algorithm based on MB-GLBP, but is higher than the state-of-the-art finger vein recognition based on PBBM and PDBM. Thus, the recognition effect of our algorithm recognition is relatively better. In addition, we encrypt the finger vein feature template to enhance the security of our algorithm, and can also change the Gbor kernel function parameters to enhance it's security, while the security of other improved finger vein recognition algorithms based on LBP often can not be guaranteed. In conclusion, our algorithm is effective and possesses higher application value in the future.

4. Conclusions.

We propose a secure finger vein recognition algorithm based on MB-GLBP and Logistic Mapping. Firstly, we extract the original vein feature data by the MB-GLBP algorithm, and then map the user's password randomly into the initial values of the Logistic mapping. After that, we use them to generate a Logistic sequence of real numbers and a Logistic binary sequence to scramble and encrypt the feature data. And finally, we accomplish the matching by computing the Euclidean distances among the final feature templates of the training samples and the testing samples.Our experimental results indicate that the new method has high security and can keep the verification rate and the EER consistent.

Acknowledgment.

This material is based upon work funded by Zhejiang Qianjiang Talents Project (2013R10071).

REFERENCES

[1] H. Luo, F. X. Yu, J. S. Pan, S. C. Chu, P. W. Tsai, A Survey of Vein Recognition Techniques, *Information Technology Journal*, vol. 9., no. 6, pp. 1142-1149, 2010.

[2] T. Ojala, M. Pietikainen, D. Harwood, A comparative study of texture measures with classification based on feature distributions, *Pattern Recognition*, vol.29, no.1, pp.51-59, 1996.

[3] K. Q. Wang, K. A. S, X. Q. Wu, Q. S. Zhao, Finger vein recognition using LBP variance with global matching, *Proceedings of 2012 International Conference on Wavelet Analysis and Pattern Recognition, ICWAPR 2012*, Xian, China, vol.2012, pp.196-200, 2012.

[4] J. L. Peng, Q. Liu, A. A. A. El-Latif, N. Wang, X. M. Niu, Finger Vein Recognition with Gabor-Wavelets and Local Binary Patterns, *IEICE Transactions on Information and Systems*, vol.96, pp.1886-1889, 2013.

[5] N. Lalithamani, M. Sabrigiriraj, Palm and hand vein-based fuzzy vault generation scheme for multi-biometric cryptosystem, *Imaging Science & Photographic Technology*, vol.63, no.2, pp.111-118, 2015.

[6] N. Dey, B. Dey, M. Biswas, D. Das, A. Chaudhuri, SS, BioHash Code Generation from Electrocardiogram Features, *Proceedings Of The 2013 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, India, pp.732-735, 2013.

[7] Q. Y. Xie, Q. Dai, Fusing Gabor and LGBP Feature for Face ecognition with One Training Image Per Person, *Journal of Chinese Computer Systems*, vol.35, no.7, pp.1655-1661, 2014.

[8] G. N. Girish, S. Naika, C. L. Das, K. Pradip, Face recognition using MB-LBP and PCA: A comparative study, *2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI 2014*, Wuhan, China, pp.1-6, 2014.

[9] W. C. Chen, M. Sabrigiriraj, The research of biometric template protection based on chaotic encryption, Ph.D. Thesis, Beijing Jiaotong University, Beijing, China, 2008.

[10] G. P. Yang, X. M. Xi, Y L. Yin, Finger Vein Recognition Based on a Personalized Best Bit Map, *Sensors*, vol.12, no.2, pp.1738-1757, 2012.

[11] X. H. Li, X. M. Xi, Y L. Yin,G. P. Yang, Finger Vein Recognition Based on a Personalized Best Bit Map, *Applied Mathematics & Information Sciences*, vol.8, no.6, pp.3121-3127, 2014.