International Journal of Hybrid Information Technology
Vol. 9, No. 5 (2016), pp. 321-330
http://dx.doi.org/10.14257/ijhit.2016.9.5.27

Study on the Encryption of Finger Vein Features Image in Mobile Internet

Zhenliang Jia

(Software Technology Vocational College, North China University of Water Resources and Electric Power, Zhengzhou 450045, China)
hennanjzl@sina.com

Abstract

Information security in mobile internet is a hot topic currently. The encryption of finger vein image is the starting point. The features of finger vein image should be extracted firstly. Then the vein image size should be obtained by constructing image smoother and the selection of light and dark areas and reinforcement of feature images are used for getting the vein feature images after collection. Secondly, the vein images are encrypted with the integrated methods using Arnold mapping based on wavelet basis function and twice Logistic mapping and Baker converting. The paper makes experimental comparison on relations analysis and differential attack analysis to describe the algorithm has features of high security and time-saving, so it suits for the promotion in the mobile internet environment completely.

Keywords*: mobile internet, finger vein feature, encryption, mobile internet*

1. Introduction

Comparing to the Internet, mobile internet is more fast and convenient in getting and spreading the information, so it's widely used by more and more people. But due to the influence [1] from network security and so on, the image encryption has been one of research directions of data encryption [2], in which finger vein image encryption is worth for attention, because it's possible to be hijacked and tampered. Domestic and foreign scholars studied the image encryption from various aspects. The literatures [3,4,6,8] proposed using Logistic mapping or chaos system to produce a set of pseudo-random sequence, finally getting encrypted images; literature [5, 7] proposed the chaotic sequence of X, Y, Z three directions based on Chen mapping construction. Experiment proves that it is feasible and effective to use the algorithm for fast image encryption.

The paper is divided into two parts. In the first part, it introduces getting the images through features by constructing image smoother and then making feature extraction against the areas light and dark of vein image to get complete vein feature image. The second part focuses on the obtained images and then applies the integrated encryption method based on wavelet basis function Arnold mapping, twice Logistic mapping and Baker converting on the vein images. The simulation experiment shows the algorithm in this paper has high security.

2. Collection and Process of Vein Image

2.1. Construct Image Smoother

The single structure of vein image cannot be transferred in mobile internet. So we need to construct image smoother to store the effective information of vein. The paper constructs 1 8 ×8 image smoother based on 4 4×4structural units, shown as Figure1.

ISSN: 1738-9968 IJHIT

0	0	0	0	1	0	0	0
1	1	1	1	0	1	0	0
1	1	1	1	0	0	1	0
0	0	0	0	0	0	0	1
0	0	0	1	0	1	1	0
0	0	1	0	0	1	1	0
0	1	0	0	0	1	1	0
1	0	0	0	0	1	1	0

Figure1. 8×8 Image Smoother

Carry out dilation operation for the vein image f by image smoother to get 4 subimages f_a, f_b, f_c, f_d and then reconstruct the image through weighting.

$$\begin{cases} f = \alpha \times f_1 + \beta \times f_2 + \kappa \times f_3 + \rho \times f_4 \\ s.t \;\; f_1 = f \oplus f_a \\ \quad f_2 = f \oplus f_b \\ \quad f_3 = f \oplus f_c \\ \quad f_4 = f \oplus f_d \end{cases} \quad (1)$$

2.2. Light and Dark Areas Extraction of Vein Image

There are light and dark areas in the vein image. To get the feature information of the areas, the paper designs a structure sequence with increasing size$\{ \varepsilon_1, \varepsilon_2, \cdots \varepsilon_i \}$. Making dilation for each unit size image to get $\varepsilon_i = \overbrace{\varepsilon_1 \oplus \varepsilon_1 \oplus \cdots \oplus \varepsilon_1}^{t} (i \le t)$. Change the unit size continuously to extract different image details. The paper adopts White top-hat and Black top-hat.

(1) Changing formula of White top-hat

$$White\,top-hat_i = f \times (1-\varepsilon_i) \quad (2)$$

$White\,top-hat_i$ refers to making the White top-hat on the i dimension for vein image f through ε_i. $White\,top-hat_{i(i-1)}$ refers to the details in the light area of vein image f size between two close sizes. The formula is shown as (3) and the extracted light area information in the vein image is shown as (4)

$$White\,top-hat_{i(i-1)} = White\,top-hat_i \cap White\,top-hat_{i-1} \quad (3)$$

$$f_W = \sum_{i=0}^{k} White\,top-hat_i \Big/ k + \sum_{i=1}^{k} White\,top-hat_{i-1} \Big/ (k-1) + \sum_{i=1}^{k} White\,top-hat_{i(i-1)} \Big/ k(k-1) \quad (4)$$

f_W means the White top-hat result of the image light area feature from dimension 0 to k.

(2)：Black top-hat transformation formula

$$Black\,top-hat_i = f \times (\varepsilon_i - 1) \quad (5)$$

$White\,top-hat_i$ refers to making the Black top-hat on the i dimension for vein image f through ε_i. $White\,top-hat_{i(i-1)}$ refers to the details in the dark area of vein image f size between two close sizes. The formula is shown as (6) and the extracted dark area information in the vein image is shown as (7)

$$Black\,top-hat_{i(i-1)} = Black\,top-hat_i \cap Black\,top-hat_{i-1} \quad (6)$$

$$f_B = \sum_{i=0}^{k} Black\ top-hat_i \Big/ k + \sum_{i=1}^{k} Black\ top-hat_{i-1} \Big/ (k-1) + \sum_{i=1}^{k} Black\ top-hat_{i(i-1)} \Big/ k(k-1) \quad (7)$$

f_B means the Black top-hat result of the image light area feature from dimension 0 to k.

2.3. The Reinforcement of Vein Image

To reinforce the effect for getting vein images, the paper maps the vein original image f, white area f_W and black area f_B in internal $[0,1]$, to get:

$$\begin{cases} \overrightarrow{f_L(x,y)} = f(x,y)/L \\ \overrightarrow{f_{WL}(x,y)} = f_W(x,y)/WL \\ \overrightarrow{f_{BL}(x,y)} = f_B(x,y)/BL \end{cases} \quad (8)$$

In formula (8), $\overrightarrow{f_L(x,y)}$, $\overrightarrow{f_{WL}(x,y)}$, $\overrightarrow{f_{BL}(x,y)}$ are the results of mapping different objects. Use enhancement operator to carry out non-linear transformation for the vein original image f_L, and the result after transformation is denoted as f_L', k is the middle critical point, shown as Figure(9)

$$f_L'(x,y) = G(f_L(x,y)) = \begin{cases} f_L(x,y)^2, & 0 \le f_L(x,y) \le k. \\ 1 - f_L(x,y)^2, & k < f_L(x,y) \le 1. \end{cases} \quad (9)$$

Use formula (10) to get the light and dark difference value of vein image, denoted as $f_{diff}(x,y)$.

$$f_{diff}(x,y) = f_{WL}(x,y) - f_{BL}(x,y) \quad (10)$$

Actually, it is not obvious to add $f_{diff}(x,y)$ and f_L'. So we need to set a coefficient s to make up the influence of the difference value. f_{en} refers to the image after enhancement, shown as formula (11).

$$f_{en}(x,y) = f_L'(x,y) + s \times f_{diff}(x,y) \quad (11)$$

2.4. Selection of Wavelet Basis Function

According to the features of the finger vein image, this paper selects wavelet basis function for processing, performing multi-scale refinement analysis for the function or signal through scaling and translation operation function, very suitable for local analysis. The vein image is divided into images with the same size through wavelet basis function with single wavelet transformation segment corresponding to them. The wavelet basis function as following:

$$h_{a,b}(x) = h\left[\frac{x-b}{a}\right] \qquad s.t\ h(x) = \cos(\frac{x}{4}) \bullet \exp(-x^2/2) \quad (12)$$

a as scale factor, b as translation factor.

3. The Encryption Based on Chaotic Vein Images

3.1. Arnolde Mapping

Using the initial value of chaotic system to iterate and displace the clear image is a kind of encryption method. This paper using the Arnold mapping method is an important component of the chaotic image encryption, and the mapping formula is as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N, x_0, y_0 \in \{0,1,2,.....N-1\} \quad (13)$$

In the formula (13), a, b are positive integer, and Arnold mapping has carried on the positive integer restrictions for two-dimensional reversible image, making originally adjacent pixels of vein images become no longer adjacent after transformation. Firstly, take random processing for the pixel value of certain point (x, y) in the vein image to get a new position, and then replace (x, y) by the point (x_{n+1}, y_{n+1}) transformed by Arnold mapping as the input value of next transformation, until the end of the iteration and replacing the image. The defect is that vein image is easily to recover after finite iterations, so the secrecy is worse.

3.2. The Transformation of 2D Logistic Mapping and Baker Transformation

$$\begin{cases} x_{n+1} = x_n + h(x_n + y_n - x_n^2) \\ y_{n+1} = y_n + h(y_n + x_n - y_n^2) \end{cases} \quad (14)$$

When $h \in [0.653, 0.686]$, Logistic is in the 2D chaotic state.

Baker mapping is a kind of data scrambling. The transformation expression of 2D continuous Baker as following (15):

$$\begin{cases} B(x_{n+1}, y_{n+1}) = k(2x_n, \frac{y_n}{2}), \quad x_n \in [0,1/2] \\ B(x_{n+1}, y_{n+1}) = k(2x_n - 1, \frac{y_n + 1}{2}), x_n \in [1/2,1] \end{cases} \quad (15)$$

In which, (x_n, y_n) records the original data position, and (x_{n+1}, y_{n+1}) records the data position after scrambling.

This paper combines the above two kinds of data exchange ways, designing a hybrid chaotic sequence constructor, in which, the secret key initial value is replaced by two-dimensional Logistic. After replacement by Bakert, the original image is carried out diffusion operation through matrix with the processed key, finally generating encrypted image, two hybrid encryption sequence as shown in figure 2.

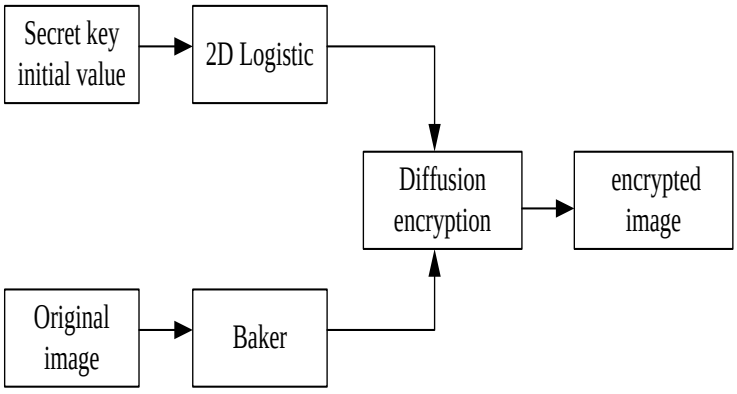

Figure 2. Mixed Encryption Sequence

4. Encryption Algorithm Design

In this paper, the design of encryption algorithm is mainly to combine the wavelet basis function, Arnold mapping, two-dimensional Logistic mapping and Baker transformation together, to carry out decomposition, replacement, diffusion and other operations to get the encryption images. The process is shown in Figure 3.

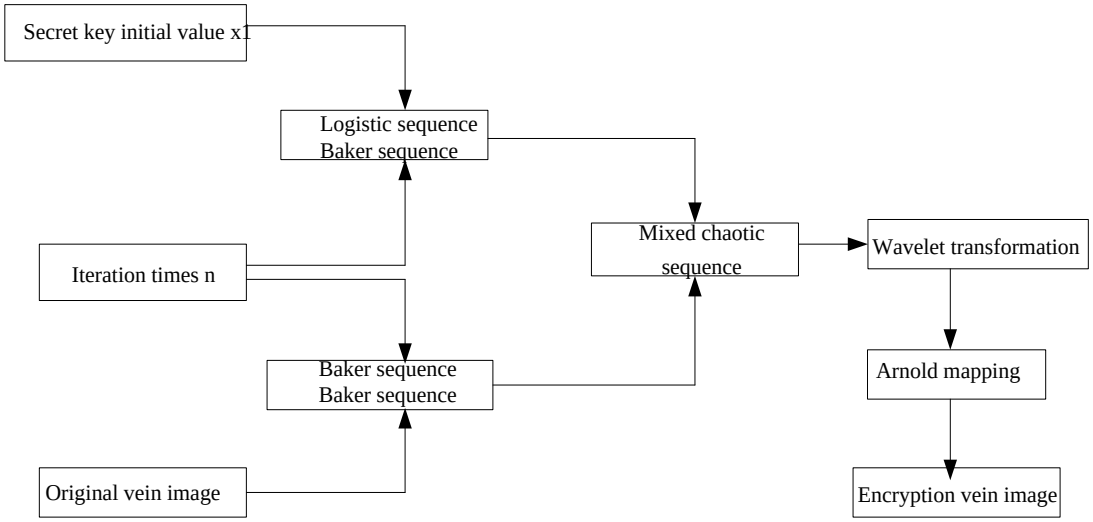

Figure 3. The Encryption Process in this Paper

Firstly, the paper divides the original vein image into matrixes $(M/4)\times(N/4)$, then generates chaotic sequence, wavelet basis function by Baker sequence and Logistic chaotic secret key and performs wavelet decomposition for the image to get decomposition coefficient matrix, adopting Arnold mapping for the decomposed matrix, which can save the calculated amount to some extent effectively, so the encryption design is reasonable.

Step 1: set a $M\times N$ vein image, and transform it into 2D matrix R, using Baker to preprocess it with n times to generate sequence X.

Step 2：For the secret key, transform $M\times N$ times through (14)iteration mapping to generate $M\times N$ pairs chaotic sequence value, with difference or B operation $B=\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n}I(M,N)$ for secret key to finish the chaotic encryption for the secret key.

Step 3: through n iterations, perform mixed chaotic sequence decomposition for the replacement image X in step 1 and sequence Y generated by Logistic secret key in step 2.

Step 4: transform the generated mixed chaotic sequence with wavelet basis function to generate sequence Z.

Step 5: use Arnold mapping Z to generate chaotic sequence to get $Z^{'}$, then replace sequence Z according to step 4 and take wavelet inverse transformation for the replaced vein image to get the final encrypted image.

5. Simulation Experiment

This paper sets up the hardware environment as internet core duo, 4GDDR3 memory, 240G hard disk capacity, and Matlabs2010 software simulation environment. Select original finger vein image, and then extract according to the vein features method described in section 1, as shown in figure 4.Based on the correlation analysis and statistical analysis, the paper verifies the effect of the finger vein image encryption, as shown in figure 4 (a - b).

Figure 4(A) Image after Collection

Figure 4(B) Image after Encryption

5.1. Correlation Analysis

Finger vein image also contains the related redundancy information as the other images. Although the image features can be extracted with the method aforesaid, the adjacent pixels cannot have certain relations independently. Select 100 pairs of adjacent pixels randomly from the collected vein images and ciphertext images, and calculate the pixels correlation of the encrypted images in horizontal direction, vertical direction and diagonal direction, in which Cov means covariance, (x, y) refers to the grey level of the adjacent pixels in the vein image, and N is the selected pixels quantity.

$$E(x) = \frac{1}{N}\sum_{k=1}^{N} x_k \quad (16)$$

$$D(x) = \frac{1}{N}\sum_{k=1}^{N} (x_k - E(x)) \quad (17)$$

$$Cov(x, y) = \frac{1}{N}\sum_{k=1}^{N} (x_k - E(x))(y_k - E(y)) \quad (18)$$

$$r(x, y) = \frac{|Cov(x, y)|}{\sqrt{D(x)\sqrt{D(y)}}} \quad (19)$$

Table 1 lists the related coefficients of two images before and after encryption by calculation, from which we can see there is high correlation between two kinds of images, indicating the collected finger vein image statistics features having been diffused to the random encryption images. Table 2 lists the comparison conditions of two images algorithms in time complexity before and after encryption, indicating the time complexity of encryption algorithm is 31.21% lower than the algorithm without encryption. Figure5-7 illustrates the compared results of two images in three directions. From the results, the encryption effect of vein image after collection is better and suitable for the encryption under mobile internet.

Table 1. The Correlation of the Adjacent Pixels of the Collected Vein Images and Encrypted Images.

Direction	Collected image	Encrypted image
horizontal direction	0. 8262	0. 0032
Vertical direction	0. 8735	0. 0027
Diagonal direction	0. 9173	0. 0024

Table 2. Time Complexity Comparison of the Collected Vein Image and Encrypted Image.

Direction(%)	Collected image(%)	Encrypted image(%)
horizontal direction	75. 25	37. 25
Vertical direction	62. 75	33. 25
Diagonal direction	89. 27	63. 14

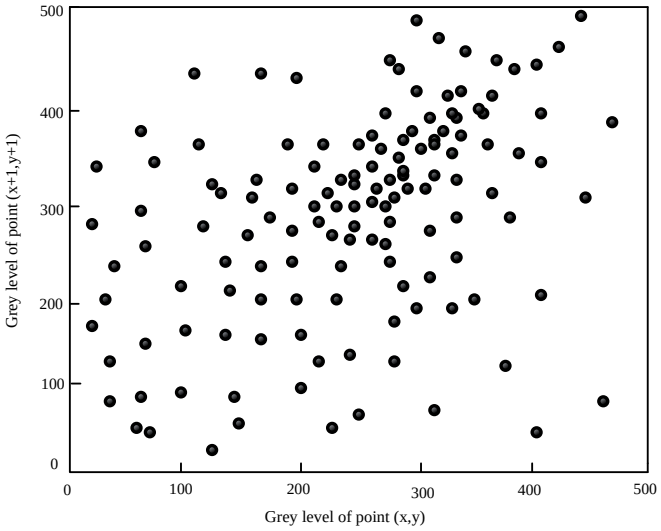

Figure5 (A). Collect Image opposite Angles

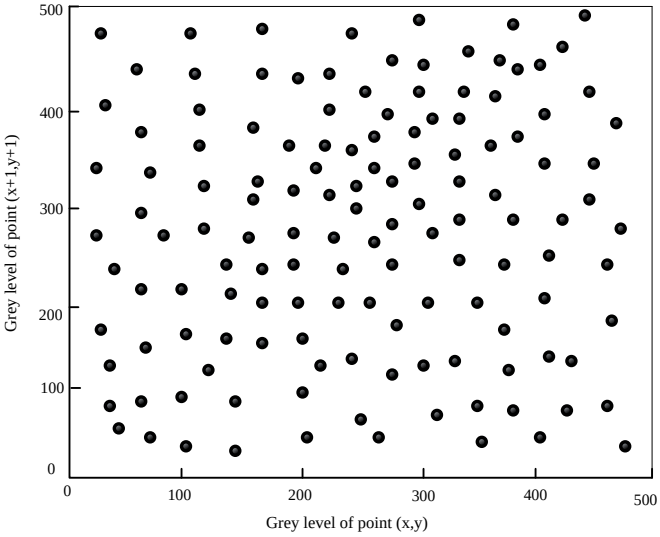

Figure 5(B). Encrypt the Image Opposite Angles

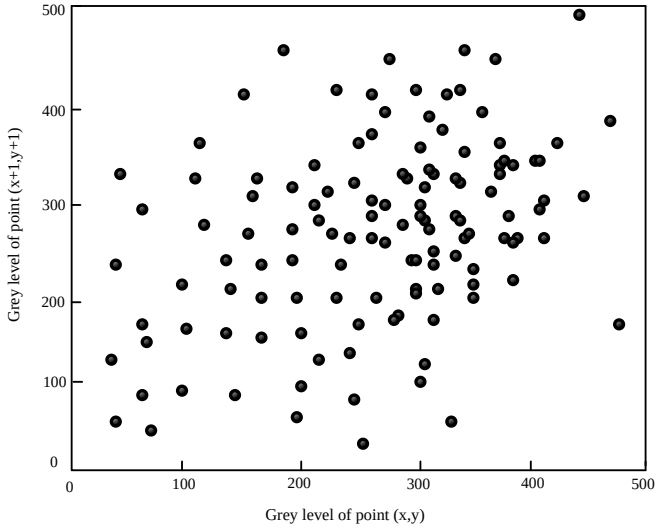

Figure 6(A). Level of Collecting Image

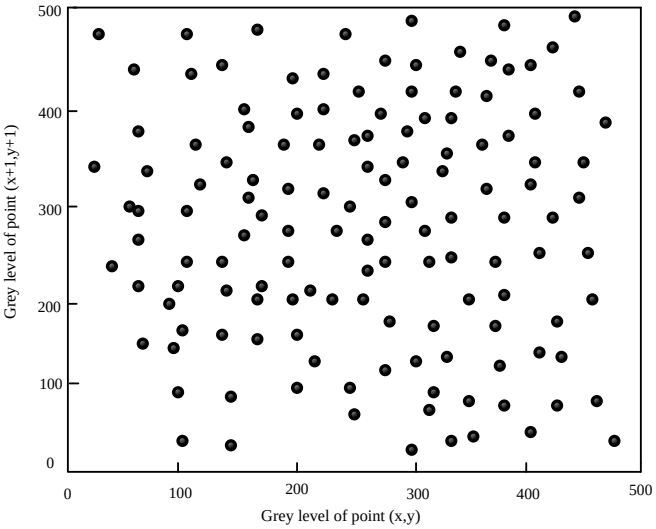

Figure 6(B). Level of Encrypted Images

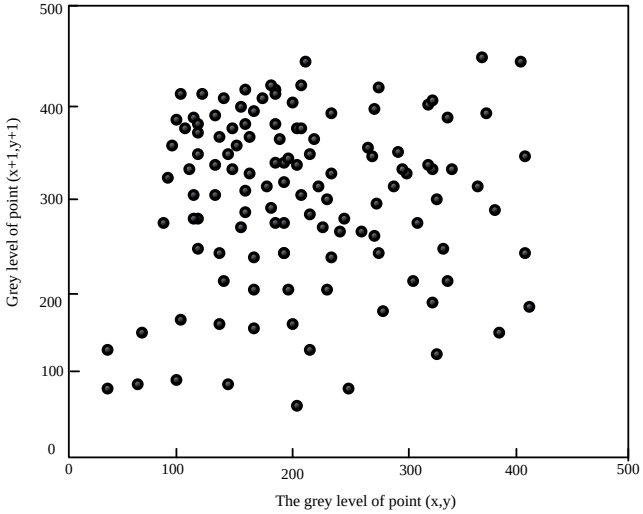

Figure 7(A). Collect Image Vertical

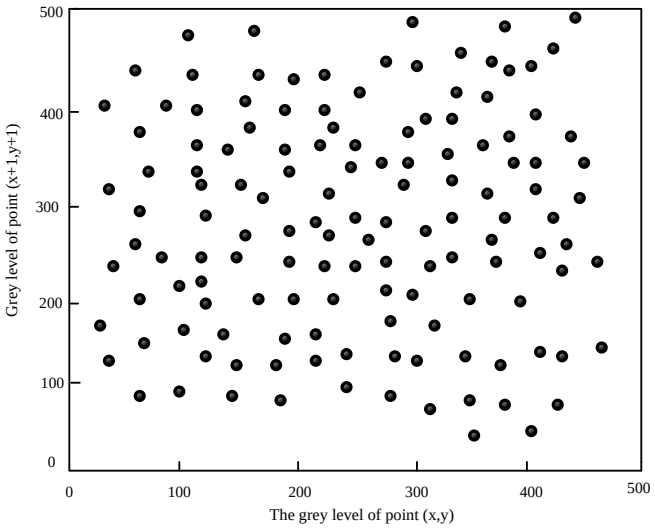

Figure 7(B). Encrypt Image Vertical

5.2. Statistic Analysis

Figure8 shows the comparison between the effect in literature [7] and the encrypted effect of the algorithm in this paper. From the figure, we can see the algorithm in this paper has better stability than the algorithm in literature [7], and the grey level is also better, which indicates that it has better effect based on Logistic combining with baker Encryption.

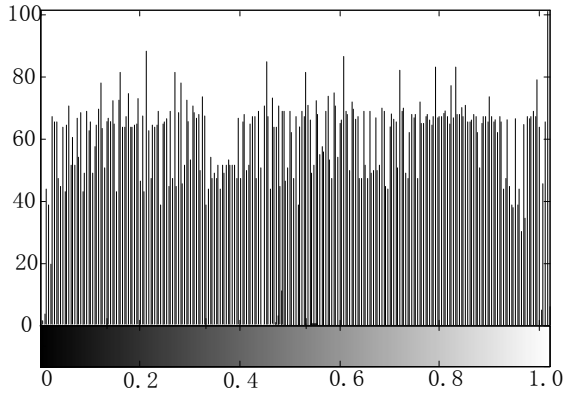

Figure 8(A). The Finger Vein Image Grey-Scale Map in Literature [7]

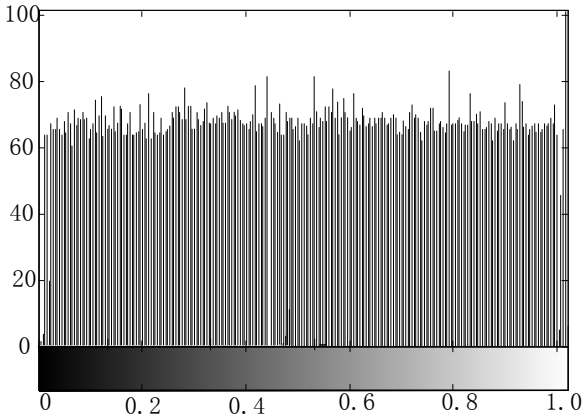

Figure 8(B). The Finger Vein Image Grey-Scale Map in this Paper

6. Conclusion

The features of finger vein image are extracted firstly. Secondly, the vein images are encrypted with the integrated methods using Arnold mapping based on wavelet basis function and twice Logistic mapping and Baker converting. The simulation experiment proves that the relation analysis and differential attack analysis have features of high security and time-saving, so it suits for the promotion in the mobile internet environment completely.

References

[1] B.Y. Fang and Y.Y. Zhang, "Analysis on Mobile Internet Application Security Issues Based on the Cloud Computing Mode", Telecommunications Science, vol. 29, no. 3, **(2013)**, pp. 41-46.
[2] C.C. Wen, Q. Wang and X.Y. Miao, "Digital Image Encryption: A Survey", Computer Science, vol. 39, no. 12, **(2012)**, pp. 6-8.
[3] B. He, H.G. Niu and L.L. Xiao, "A New 2-D Image Encryption Algorithm Based on Dual Transform", Optical Technique, vol. 41, no. 1, **(2015)**, pp. 52-58.
[4] S. Wang, W. Sun and Y.N. Guo, "Design and Analysis of Fast Image Encryption Algorithm Based on Multiple Chaotic Systems", Application Research of Computers, vol. 32, no. 2, **(2015)**, pp. 512-515.
[5] P. Peng, L.X. Sun and T.Z. Wang, "Image Encryption Method Based on Chen Chaos Mappingand Bit Plane", Mathematics in Practice and Theory, vol. 45, no. 3, **(2015)**, pp. 117-122.
[6] B. Xu and L. Yuan, "Research on Image Encryption Algorithm Logistic Chaotic Based on an Improved

Digital Mapping", Computer Measurement & Control, vol. 22, no. 7, **(2014)**, pp. 2157-2159.
[7] Q.J. Li and Y.N. Zhang, "Image Fast Encryption Algorithm Based on Chaotic Map", Computer Measurement & Control, vol. 22, no. 10, **(2014)**, pp. 3270-3273.
[8] W.K. Ding, Y. Zhang and X.L. Zhai, "Color Image Compression and Encryption Algorithm Based on Self-adaption and Multiple Chaotic Systems", Journal of Henan University (Natural Science), vol. 45, no. 2, **(2015)**, pp. 223-228.

Authors

Zhenliang Jia (1976.03-), She is aLecturer, Master, Research Orientation: Computing Network.

