An Improved Cancelable Fingerprint Template Encryption System Research

Feng Wang, Bo Han, Lei Niu and Ya Wang
School of Computer and Information Engineering, Fu Yang Teachers College,
Fu Yang 236037, Anhui- P.R.China
[e-mail: wffync@fync.edu.cn]
*Corresponding author: Feng Wang

Received May 27, 2016; revised September 30, 2016; accepted October 24, 2016; published April 30, 2017

Abstract

For the existing security problem based on Fuzzy Vault algorithm, we propose a cancelable fingerprint template encryption scheme in this paper. The main idea is to firstly construct an irreversible transformation function, and then apply the function to transform the original template and template information is stored after conversion. Experimental results show it effectively prevents the attack from fingerprint template data and improves security of the system by using minutiae descriptor to encrypt abscissa of the vault.

The experiment uses public FVC2004 fingerprint database to test, result shows that although the recognition rate of the proposed algorithm is slightly lower than the original program, but the improved algorithm security and complexity are better, and therefore the proposed algorithm is feasible in general.

Keywords: Fuzzy Vault; cancelable fingerprint template, encryption, irreversible transformation function, minutiae descriptor

This work is supported by Natural Science Foundation Key project of Anhui Provincial Education Department (No.KJ2015A295, KJ2015A278), National Natural Science Foundation of China under Grant No. 61401101, and Natural Science Foundation of Anhui Province under Grant No. 1408085QF122. Natural Science Foundation project of Anhui Provincial Education Department (No. 2015KJ014).

https://doi.org/10.3837/tiis.2017.04.022 **ISSN : 1976-7277**

1. Introduction

Compared with traditional authentication technology, although the current fingerprint identification system basically reaches the practical requirement on the recognition accuracy and speed, but there are still some deficiencies in template security issue. The current fingerprint identification system mainly uses minutiae as recognition feature, and the specific details of the information are stored as the bare data in the system, without the use of any encryption. With the development of cracking technology, the entire fingerprint identification system will be fully exposed to hackers attacking range, thus threatening the security of the user identity. Cappelli et al.[1] research has shown it can recover the original fingerprint image according to the number of minutiae and direction, location. **Fig. 1** shows how to reconstruct the fingerprint image based on minutiae.

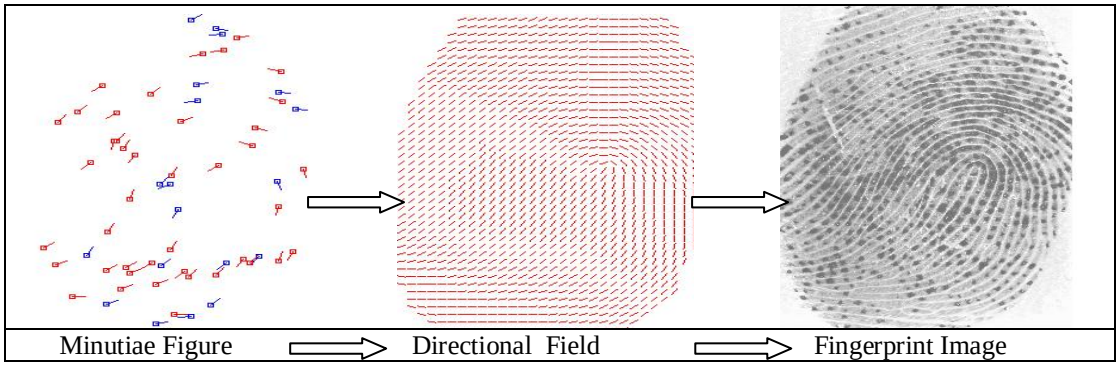


Fig. 1. Reconstructing the fingerprint image from minutiae template

Through the study of the current biometric template protection of technological development, since the authentication system is vulnerable to be attacked, Anil K.Jain et al [2] proposed that an ideal biometric template protection program should have the following characteristics:

(1) Security: an attacker cannot recover the original template from the conversion template data.

(2) Diversity: security templates can avoid cross-matching attack between multiple databases.

(3)Reversibility: When a user needs to revoke the original template and publish a new template, it does not expose the original biometric information.

(4)Certified Performance: certification performance of biometric template protection scheme cannot fall too much.

Biometric encryption technology can effectively solve this problem which combines biometrics and cryptography advantages, it not only uses biometric features to manage keys, the but also uses a key to protect biometric information, so the security of biometric data and the key has greatly been improved[3], it finds a balance between the fuzziness of biological information and cryptography accuracy. In biometric encryption technology, the key with biometric data in order to generate helper data and is stored in the system database [4]. Auxiliary biometric data has played a significant role for solving encryption technology. In registration phase, the system will generate the users encryption based on biometric

information, and has a certain fault tolerance. Legitimate users can restore their own biometric key from the helper data in certification stage.

Algorithm proposed by Soutar et al[5] is one of the oldest in the field of practical algorithm in 1998, on the base of Fourier transform and image processing, the algorithm main process is divided into encryption and decryption, in registration phase binding randomly the users fingerprint characteristics and the key, it will be released only when the authentication key is success, but critics argue that the algorithm can not guarantee a good system security. Juels et al [6] proposed a fuzzy commitment program in 1999, which is a typical key binding scheme from basic cryptography bit commitment scheme; it combines with biometric identification technology and error correction code technology. On the basis of the fuzzy commitment scheme Hao et al.[7] realized a iris encryption scheme in 2006, the program uses a two-factor authentication and combines with cryptography ideas, making system fault tolerant more stronger, if it want to be verified successfully only when the iris and token of legitimate users are provided simultaneously. Juels and Sudan[8] proposed fuzzy vault program in 2003, which is most classic practical program in the field of biometric encryption, it is well to combine with biometric fuzziness and key accuracy, since it is able to handle the error between the sets, it is particularly suitable for the biometric data, such as fingerprints. Clancy et al [9] proposed a fingerprint vault program based on fuzzy vault program in 2003 and specifically described the implementation of fuzzy vault in fingerprint domain, while its disadvantage is that the fingerprint images previously used in the experiment must register manually. Yang et al. [10] proposed a fuzzy fingerprint vault in 2005, the program uses the singular point for registration based on the minutiae structure. In the same year Uludag et al.[11] proposed a more practical and feasible fuzzy vault for fingerprint, its basic idea is basically the same fingerprint vault, but there is only difference in details. All the above mentioned method of fingerprint images are artificially registration, for the first time in 2006 Uludag[12] used the computer for registering fingerprint image in an encrypted domain. Nandakumar et al.[13] proposed to add a layer password in system peripherals in 2007, and stored minutiae parameter in the template after irreversible function transformation, which makes the system have two layer protection, the system security has been greatly improved. Jesse et al.[14] experimental result shows that fuzzy vault on fingerprint recognition is feasible by analyzing the fuzzy vault security in 2013.

In domestic, there are many researchers have depth study in biometric encryption, Li P et al. [15] in 2008 proposed a cancelable fingerprint template implementation program and had carried out experiments. Li Peng et al.[16] in 2009 summarized the development of biometric template protection technology and carried out a detailed classification. In 2011, by analyzing problems existing in cross comparison of fingerprints fuzzy vault, ZHANG Rong-lin et al.[17] proposed an improved two factor cancelable fuzzy vault program and improved the security of the system. At present, many researchers have depth study on the fuzzy vault and successfully applied it to the face, fingerprint, signature, iris biometrics and so on.

2. Fingerprint Image preprocessing

Since the entire encryption system requires the use of the fingerprint image minutiae, so accurate extraction minutiae feature plays a vital role in recognition performance, extracting minutiae mainly includes the following aspects, the flowchart as the **Fig. 2** shows, The minutiae extraction process is shown in **Fig. 3**

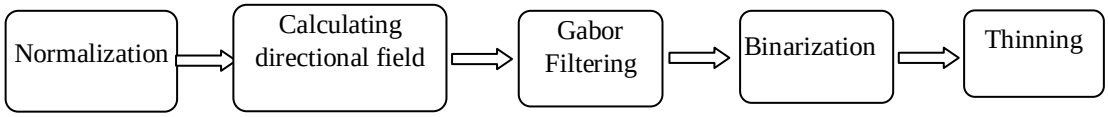


Fig. 2. fingerprint image preprocessing flowchart

2.1 Normalization

Because the quality of fingerprint images captured by fingerprint scanner is influenced by many factors, such as dryness and wetness of finger, cleanness of scanner and dryness and wetness of the weather, we firstly use normalization to remove the effects of sensor noise and finger pressure difference:

$$G(i,j)=\begin{cases} Mean_0 + \sqrt{\dfrac{Var_0 * (I(i,j)-Mean)^2}{Var}}, if I(i,j) > Mean \\ Mean_0 - \sqrt{\dfrac{Var_0 * (I(i,j)-Mean)^2}{Var}}, otherwise \end{cases} \quad 2\text{-}1$$

$$Mean=\frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}I(i,j) \quad 2\text{-}2$$

$$Var=\frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I(i,j)-Mean)^2$$

Where $Mean_0, Var_0$ are the desired mean and variance value, we can conclude that normalization improve the full image contrast and not change fingerprint valleys quality.

2.2 Computing orientation field

Fingerprint orientation field reflects true texture features of the fingerprint image, indicating the fingerprint ridge direction. Currently there are a lot of methods to obtain fingerprint orientation field, we use the literature [18] method to compute and smoothed. The steps are as follows:

(1)We divide the fingerprint image into w * w blocks of size and calculate the gradient of each pixel which is calculated to use Sobel operator (w=8).

(2)Calculating each block direction as the formula

$$V_x(i,j)=\sum_{i-\frac{W}{2}}^{i+\frac{W}{2}}\sum_{j-\frac{W}{2}}^{j+\frac{W}{2}}2\partial_x(u,v)\partial_y(u,v) \quad 2\text{-}3$$

$$V_y(i,j)=\sum_{i-\frac{W}{2}}^{i+\frac{W}{2}}\sum_{j-\frac{W}{2}}^{j+\frac{W}{2}}\partial_x{}^2(u,v)-\partial_y{}^2(u,v) \quad 2\text{-}4$$

$$\theta(x,y)=\frac{1}{2}\arctan\frac{V_y(i,j)}{V_x(i,j)} \quad 2\text{-}5$$

Where θ(x,y) is perpendicular to the main direction of the W*W window Fourier frequency.

(3)Filtering: The above orientation field in some areas is not accurate enough due to noise, the impact of disconnection. According to fingerprint ridge changing slowly characteristics (except pattern area), we use a low pass filter for smoothing orientation field. Firstly, we use formula $\phi_x = \cos(2\theta(i,j)), \phi_y = \sin(2\theta(i,j))$ to transform the orientation field into a continuous vector field, the following is filtering:

$$\phi'_x(x,y) = \sum_{-\frac{h}{2}}^{\frac{h}{2}} \sum_{-\frac{h}{2}}^{\frac{h}{2}} \left(l(u,v) \phi_x(i-uh, j-vh) \right) \quad 2\text{-}6$$

$$\phi'_y(x,y) = \sum_{-\frac{h}{2}}^{\frac{h}{2}} \sum_{-\frac{h}{2}}^{\frac{h}{2}} \left(l(u,v) \phi_x(i-uh, j-vh) \right) \quad 2\text{-}7$$

h is a two-dimensional low-pass filter, l (u, v) is the weight value of each point of the filter. Finally we get a smooth block orientation field below:

$$O(i,j) = \frac{1}{2} \arctan \frac{\phi'_y(i,j)}{\phi'_x(i,j)} \quad 2\text{-}8$$

2.3 Gabor function enhancement

After completing the above steps, we can construct a Gabor function. Gabor filter can separated from adhesions fingerprints and reconnect broken fingerprint due to the good frequency domain and direction selectivity. L.Hong etc [19] firstly applied it on the fingerprint enhancement and achieved good results. The following is a two-dimensional Gabor function:

$$G(x,y,\theta,f_0) = \exp\left\{ -\frac{1}{2} \left(\frac{x_\theta^{\,2}}{\sigma_x^{\,2}} + \frac{y_\theta^{\,2}}{\sigma_y^{\,2}} \right) \right\} * \cos(2\pi f_0 x) \quad 2\text{-}9$$

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad 2\text{-}10$$

f_0 is ridge frequency, x, y are the coordinates of corresponding two-dimensional template, θ is ridge orientation, σ_x, σ_y respectively are the Gaussian enveloping constant along the horizontal axis and the vertical axis. x_θ, y_θ respectively are the distances between certain element of enhanced template and the center line.

defining formula(9) as $\sigma_x=\sigma_y$, defining formula (10) as θ=0

$$G(x,y,f_0)_{\theta=0} = \exp\left\{ -\frac{1}{2} \left(\frac{x^2}{\sigma_x^{\,2}} \right) \right\} * \exp\left\{ -\frac{1}{2} \left(\frac{y^2}{\sigma_y^{\,2}} \right) \right\} * \cos(2\pi f_0 y) \quad 2\text{-}11$$

the above formula is divided into the following forms:

$$G(x,y,f_0)_{\theta=0} = G_L G_B \quad 2\text{-}12$$

$$G_L(x,f_0) = \exp\left\{ -\frac{1}{2} \left(\frac{x^2}{\sigma_x^{\,2}} \right) \right\} \quad 2\text{-}13$$

$$G_B(y, f_0) = \exp\left\{-\frac{1}{2}\left(\frac{y^2}{\sigma_x^2}\right)\right\}\cos(2\pi f_0 y) \qquad 2\text{-}14$$

G_L (x, f_0) and G_B (y, f_0) respectively are along the ridge directional low-pass filter and the vertical ridge directional band-pass filter. The horizontal filter corresponds to the ridge directional pixels weighted average so it can smooth the fingerprint and play the role of a broken connection. The vertical filter enable the ridges and valleys higher contrast by making around the current point positive, a little further negative.

2.4 Binarization

Fingerprint image binarization is that the gray image is transformed into a 0-1sequence binary image, its aim is to retain the main ridge information, save a lot of space and remove breakpoints. In binary image, the fingerprint ridge becomes 1, valley line goes 0, and assuming ridges and valleys in the image size roughly the same proportion, specific formula as shown in 2-15:

$$P(m, n) = \begin{cases} 255 \cdots\cdots I(m, n) > Mean \\ 0 \cdots\cdots others \end{cases} \qquad 2\text{-}15$$

2.5 Thinning

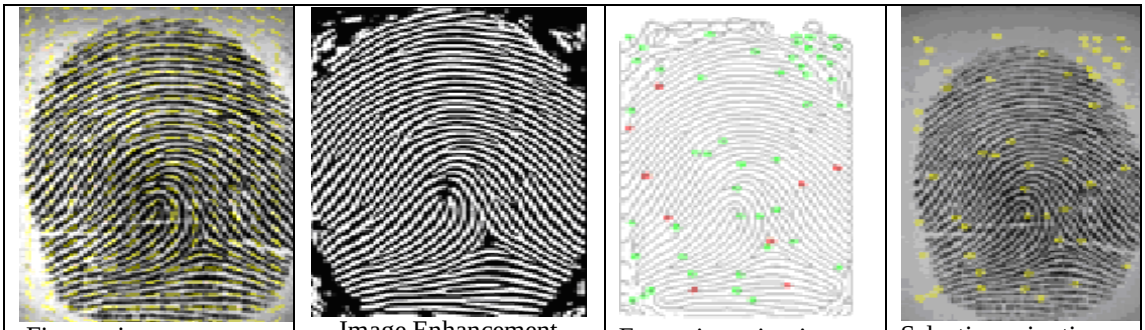
After obtaining binary fingerprint image, deleting its edge pixels makes it become one pixel width skeleton image. A good thinning algorithm generally satisfy retention, convergence, fast, topological properties requirement, specific thinning algorithm steps are as follows:

①traversing fingerprint image to find the boundary points.

②for boundary point P, defining two feature vectors nsum and tsum

$nsum = \sum_{i=1}^{8} p_i$, $tsum = \sum_{i=1}^{8} |p_{i+1} - p_i|$ where $p_9 = p_1$, If point p meets simultaneously $tsum = 2, nsum! = 1, nsum < 6$, deleting it.

③continuing to look to the next border point, until there is no boundary points can be deleted



Fingerprint pattern | Image Enhancement | Extraction minutiae | Selecting minutiae

Fig. 3. Extraction minutiae

3. Improved Fuzzy Vault Cancelable fingerprint algorithm

3.1 Problems of traditional algorithm

Although fuzzy vault program solves contradiction between the biometric ambiguity and cryptography accuracy, however, the program still exist many problems:

(1) Since the fuzzy vault template matching is performed in the encryption domain, so the recognition rate will decline;

(2)Since the template is stored after conversion, so the encrypted domain registration is a problem;

(3)There is multiple database cross-reference vulnerability; an intruder can attack by brute force.

So it is feasible to improve fuzzy vault framework, we fuse minutia descriptor into encrypt fuzzy vault the abscissa value, and saving it as helper data in the system, and then using transform function to transfer minutiae coordinate value irreversibly which is proposed by Ratha et al.[20], finally we use the fuzzy vault algorithm for encryption.

3.2 template conversion based on Butter Worth kernel function

The feature of Butterworth function is the frequency response curve maximum flat and without ups and downs within pass band-width, and in the suppressed frequency band it is gradually reduced to zero. The logarithm of the amplitude increases with the angular frequency decreases gradually, and tending to negative infinity.

Template deformation technique is to obtain maintaining similar biometric features template through the original template some parameters irreversible transformation. Since it can generate new transformation template by changing some parameters, the template is cancelable.

Because there will be some error between the two fingerprint templates, and therefore generally matching will have a certain tolerance to the error, it may cause to have a incorrect match between the canceling template and the newly registered template, in order to avoid this situation, we use an irreversible function to transform original fingerprint template, which aims to launch the feature points outside the error tolerance range of the system. Firstly, we assume minutiae coordinates $p(x, y, \theta)$, making p point moving a certain length K along the direction of $\psi(x, y)$, then adding displacement $T(x, y)$, around P point whirling a fixed random angle α_{rand}, and then adding a angle $\beta(x, y)$, minutiae coordinate is $p'(x', y', \theta')$.

$$x' = x + K\cos\left(\psi(x, y)\right) + T(x, y) \quad 3\text{-}1$$

$$y' = y + K\sin\left(\psi(x, y)\right) + T(x, y) \quad 3\text{-}2$$

$$\theta' = \mathrm{mod}\left(\theta + \beta(x, y) + \alpha_{rand}, 2\pi\right) \quad 3\text{-}3$$

$$T(x, y) = \sum_{i=1}^{N_T} \frac{T_i}{1 + \left[D_{(x_i y_i)}(x, y) / D_{T_0}\right]^{2n_1}} \quad 3\text{-}4$$

$$\psi(x,y) = \sum_{j=1}^{N_\beta} \frac{(-1)^{rand01(j)}\beta_j}{1+\left[D_{(x_j y_j)}(x,y) / D_{\beta_0}\right]^{2n_2}} \quad 3\text{-}5$$

$$\alpha(x,y) = \sum_{k=1}^{N_\alpha} \frac{(-1)^{rand01(j)}\alpha_k}{1+\left[D_{(x_k y_k)}(x,y) / D_{\alpha_0}\right]^{2n_3}} \quad 3\text{-}6$$

$D_{(x_i y_i)}(x,y)$ is the distance between point (x,y) and point (x_i, y_i), $(x_i, y_i), (x_j, y_j), (x_k, y_k)$ are some random points in the flat, D_{r_0}, D_{β_0}, D_{α_0} are constants, T_i, β_j, α_k respectively determine the additional displacement, the displacement direction and the magnitude of rotation angle, rand0l represents 0 or 1 randomly generated

The method of fingerprint template protection is to store the original fingerprint template information after some irreversible function transformation. However, there is no decision on how to choose the appropriate transform function. But there are some basic requirements: transformation function should be the global non-linear and has irreversibility.

In 2007, Ratha et al. proposed and analyzed three irreversible transforms for the production of revocable fingerprint templates. These transform functions are Cartesian coordinate transformation, polar coordinate transformation and function transformation. The raw fingerprint minutiae can still be matched using the minutiae matcher after these functions transformations. In the Cartesian coordinate transformation, the fingerprint image is represented as a rectangular grid, and then each lattice is transferred to another grid in the grid according to the transformation set formed by the user specific key. If the grid contains minutiae points, the coordinate values of the minutiae in the grid change as the grid moves. Polar coordinate transformation is similar to Cartesian coordinate transformation, it firstly establishes the polar coordinate system with the center point as the midpoint and the direction of the center point as the positive direction, then divides the fingerprint image into many segments, and each segment is divided into many small blocks. So the generation of the transformation vector from the key is required to set some limits so that the distance is small between the small block transformation before and after.

3.3 Based on minutiae descriptor encryption protection

3.3.1 Minutia descriptor

Minutia descriptor has a rotating and moving invariance which contains the details of the minutiae direction information. Feng[21] presented the details of minutia descriptor based on the texture, it contains the frequency and direction information which is distributed on the ring of the minutiae as the center point. Supposing the radius of the first round of is rl, there is the number of Kl sample points on the circle.

Minutiae position as the origin coordinates, minutiae direction as a positive direction to establish a polar coordinate system, the first kth sample point definition of the lth circle is:

$$\begin{cases} \rho_{l,k} = r_l \\ \theta_{l,k} = \dfrac{2\pi k}{K_l} \end{cases} \quad 3\text{-}7$$

Supposing the angle of minutiae is $\alpha\left(-\pi \le \alpha \le \pi\right)$, direction near the sample point is $\alpha_{l,k}\left(-\pi/2 \le \alpha_{l,k} \le \pi/2\right)$, Frequency is $1/w_{l,k}$, $\beta_{l,k} = \lambda\left(\alpha_{l,k} - \alpha\right)$ is $\alpha_{l,k}$ relative to α angle, and then the minutia descriptor can use the following formula:

$$D(p) = \left\{\left(\beta_{l,k}, w_{l,k}\right)_{k=0}^{K_l-1}\right\}_{l=0}^{L-1} \quad 3\text{-}8$$

It can be understood as a combination of descriptors Df (p) based on frequency and Do (p) based on direction:

$$D_f(p) = \left\{\left(w_{l,k}\right)_{k=0}^{K_l-1}\right\}_{l=0}^{L-1} \quad 3\text{-}9$$

$$D_o(p) = \left\{\left(\beta_{l,k}\right)_{k=0}^{K_l-1}\right\}_{l=0}^{L-1} \quad 3\text{-}10$$

3.3.2 Encryption based on minutiae descriptor

Fuzzy Vault security of the algorithm depends on two aspects: ①finding the real point of difficulty from the hash point; ②according to the coordinate of vault reconstructing secret polynomial, so it can effectively improve the security of the algorithm for encrypting minutiae coordinate after template transformation. Here are the specific steps of a minutia descriptor to encrypt the abscissa of the safe vault as shown **Fig. 4.**

(l)After successfully extracting minutiae, according to the formula (3-7) - (3-10) extracting corresponding minutia descriptor. A minutia descriptor contains most of the information around the vicinity of the minutiae sample point (such as the ridge direction and ridge frequency), these sample points evenly are distributed to the minutiae as the centre of a circle, with 25, 40, 60, 80 pixels for the radius on four concentric circles, each circle distributes 10, 15, 20, 30 points, a total of 75 sample points

(2)Quantizing direction value of minutia descriptor as 5-bit binary number, quantizing frequency value as four binary numbers, a total of 75 sample points can obtain 675 (75 × (5 + 4)) bits binary number, then choosing the previous 500 binary

(3)Converting the abscissa of the safe vault into 16 binary, and then BCH coding, finally get 500 binary numbers v

(4) XOR operation d with v, you can get the encrypted abscissa value.

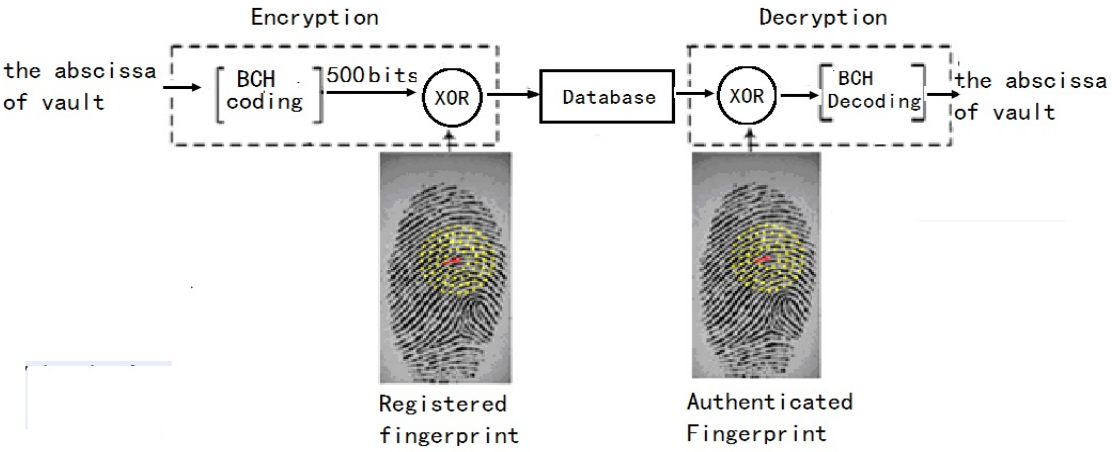


Fig. 4. Minutia descriptor for the abscissa encryption

3.4 Improved Fuzzy Vault algorithm flow

Registration phase: After obtaining a legitimate user fingerprint template, the system does not store the original fingerprint template directly, but the original fingerprint template is converted into transformation template by using a set of irreversible function, and then using fuzzy vault encryption algorithm for transformed fingerprint template and 128 randomly generated keys to encrypt so as to obtain a safe vault, and then combining with minutiae descriptor to encrypt the abscissa of safe vault minutia. Finally, the minutia abscissa set and the encrypted abscissa value as helper data are stored in the database. Specific fingerprint features encryption system is as follows **Fig. 5**:

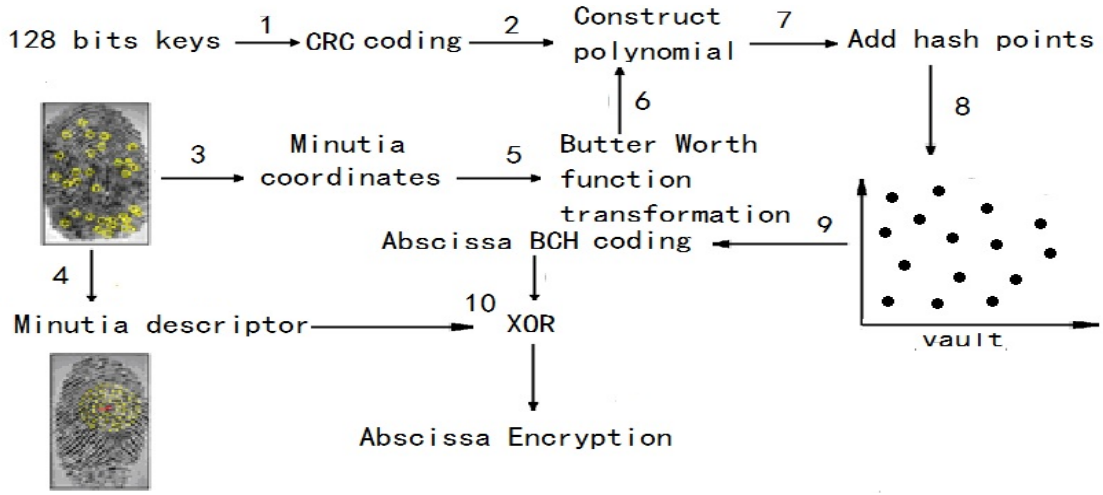


Fig. 5. Improved Fuzzy Vault fingerprint algorithm encryption process

(1)Randomly generating 128 binary number as the key S

(2)Using cyclic redundancy check (CRC) to deal with the key S so as to obtain the 16-bit binary checksum, and it will be added to the end of the S to get 144 bits key SC

(3)Constructing coding polynomial F(u). Since the length S is 128 bits, in the Galois field GF (216) the order of F(u) should be 8 bits(128/16). Dividing 144 bits of SC into the 9 parts in Galois field GF, each part is 16 bits binary number, and this nine numbers is converted to decimal as polynomial coefficients $(s_{i-1}, s_{i-2}, \cdots, s_0)$, Thereby obtaining polynomial $F(u) = s_8 u^8 + s_7 u^7 + \cdots + s_1 u + s_0$

(4) In accordance with formula (2-1)-(2-15) given normalization, image enhancement, binarization and thinning and so on, and then extracting the fingerprint minutiae feature information, where x is row minutia in the fingerprint image, y is the column minutia in the fingerprint image, H is the minutiae direction along the ridge tangent.

(5)According to the formula(3-7)-(3-10) extracting minutiae corresponding minutia descriptor in order to obtain the minutia ridge frequency and ridge direction information near 75 sample points.

(6) According to the formula (3-1)-(3-6) transformation function it irreversibly transforms the original fingerprint template minutiae (x, y, θ).

(7) After the function transformation, the minutiae (x, y, θ) information cascades the coordinate value which the coordinate values are converted to 8-bit binary number, then synthesized a 16-bit binary number, and then converted into a decimal number u again. Each cascade value of minutiae coordinate is substituted into step (3) polynomial to get corresponding abscissa value v, so the real point (u, v) of vault is obtained by step (3).

(8) Adding some hash points, point set including hash points and real points is stored in a safe vault. Hash points quantity and generating method will seriously affect the security of the system, in order to prevent an attacker to filter the hash point by comparing, the number of hash points should be far greater than the number of real points. In addition, hash points added on the function transformed template should be evenly distributed and avoid colliding between hash points and the real points.

(9)Converting the abscissa value of safe vault into 16-bit binary, and then BCH coding, finally 500 binary number v' is obtained.

(10)Quantizing direction value of minutia descriptor as 5-bit binary number, frequency value quantizing as four binary number, a total of 75 sample points can obtain 675 bits binary number, Then choosing the previous 500 binary, the d with v XOR operation, you can get encrypting abscissa value.

Authentication phase (**Fig. 6**.): The system retrieves the user live fingerprint sample, through the pretreatment whose phase is the same as encryption to give the minutia set, Then use the same template parameter for minutiae sets to template transformation, transformed minutia is obtained, and finally matching these minutia with the real point of fuzzy vault. Since the process there will be noise in fingerprint samples, so the user can not find out all the real point, but as long to find the enough real point, the polynomial can be reconstructed to obtain secret key.

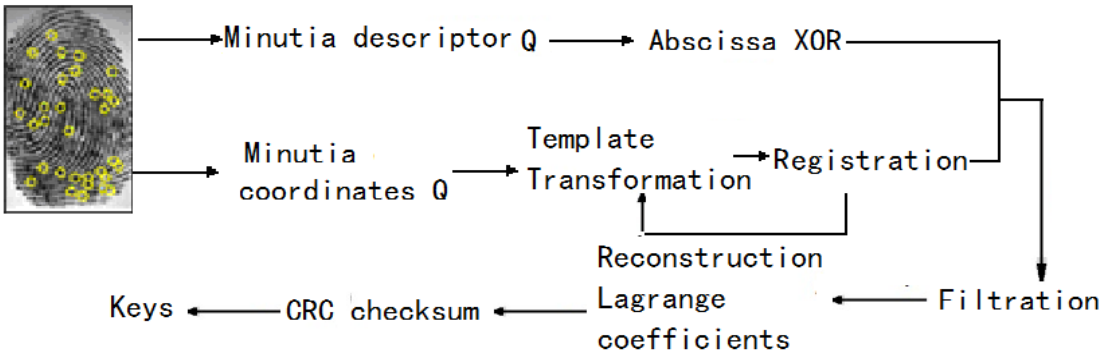


Fig. 6. Fingerprint fuzzy vault decryption process

4. Experimental results and Analysis

4.1 Relevant indicators

False Accept Rate: it is statistically false match probability of occurrence, mainly refers to the false match mistaken for true match.

False Refuse Rate: it is statistically non-match error probability of occurrence, mainly refers to the true match to be mistaken for a false match. Herein, FTC (Failure to capture errors) will be classified as FRR error, rather than as a separate evaluation criteria.

The FRR and FAR two parameters affects each other, they can be controlled by setting parameters, and can be adjusted according to the occasion demand.

In this paper, the database uses public mainstream fingerprint FVC2004 DB2, it contains 100 fingers samples collected by optical acquisition instrument, and each finger image captures eight images, a total of 800 images. Te fingerprint image size is 560 × 296, the image resolution is 569dpi, image quality is better.

4.2 Experimental results and analysis

Selecting experimental parameters as follows: the number of secret polynomial is 8; key length S is 128 bits, supposing $N_T = N_\beta = 20, N_\alpha = 5, D_{t_0} = D_{\beta_0} = D_{\alpha_0} = 18, n_1 = n_2 = n_3 = 2, K = 24$, in registration phrase, the number of selected minutiae n = 20, adding the number of hash points c = 200 (the hash points number is about ten times the real points number), the minimum distance between any two hash points d =10, the minimum distance between the real point and the hash point t = 15, the minimum distance between query minutiae and registration minutiae l = 25; in the registration process, due to fingerprint images in the collection there will be a rotation angle and the translation distance, so minutiae rotation range is set to [30, 50] degrees, and then carried out to move 10 times respectively in the coordinates x and y-axis direction.

Fig. 7 shows the fingerprint template encryption process, in (C) the red dot is the real point of the fingerprint image, and the blue dot is added hash points.

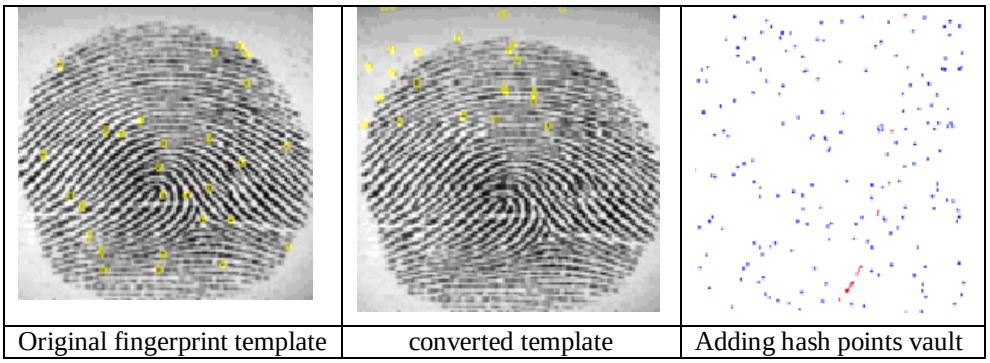


Fig. 7. The fingerprint template encryption process

Decryption phrase, you need to enter to be authenticated fingerprint image, the experiment will choose a fingerprint database in the same fingerprint authentication image, the same procedure will be executed for preprocessing operation, extracting minutiae coordinate and minutia descriptor, then using irreversible transformation function to transform template. finally we use the transformed fingerprint template to align, and loop these two steps repeatedly, which minutiae angle range [30 50] degrees of rotation and is carried out 10 times simultaneously to move in the x and y axis direction, selecting the maximum points set D. we use a selected point set D and certified fingerprint minutiae template descriptors to execute BCH-decoding in order to obtain about ten points sets, the polynomial is reconstructed by using Lagrange interpolation and point set D, lastly we use cyclic redundancy check to check code, key S will be restored if the code is correct.

Table 4-1 shows the experimental results to compare with and the literature [12] and [20] experimental results, in which the polynomial order n = 8, the number of hash points is 200

Table 4-1. the Key Length Experimental Results Contrast

Key Length(bit)	The proposed algorithm		Literature[12] algorithm		Literature [20] algorithm	
	FRR	FAR	FRR	FAR	FRR	FAR
96	11%	0	9%	0.13%	12%	0
128	10%	0	9%	0.01%	13%	0
160	15%	0	14%	0	23%	0

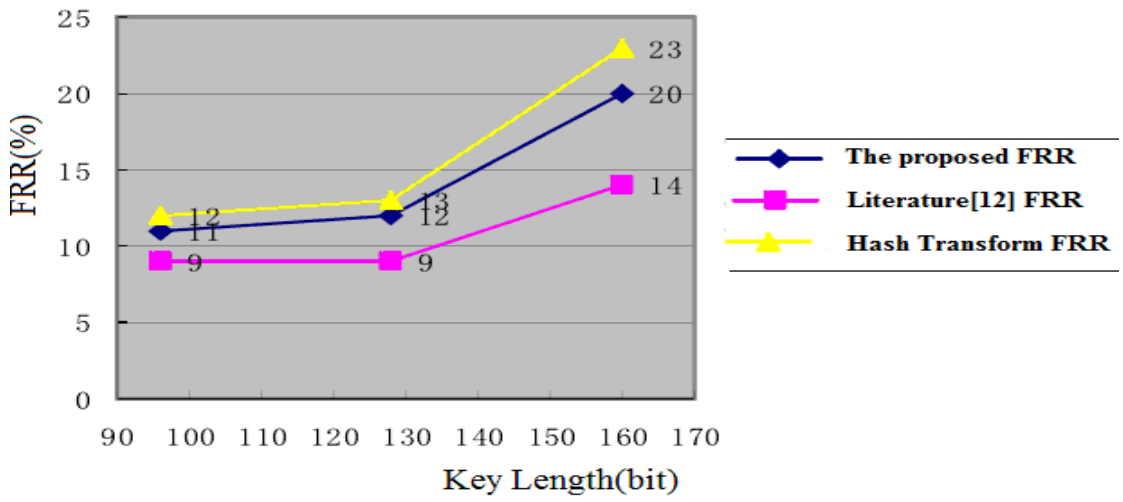


Fig. 8. Key lengths affects experimental results contrast

The security has a certain improvement after converting the original template, a successful match probability is extremely after different template are converted, and for the fingerprint template protection, the lower the FAR, the security is higher.

From **Fig. 8** we can see from the experimental results that the proposed algorithm FRR is lower than the literature [20] and higher than the literature [12], but the three algorithms FRR is higher than the original program, whose reason is not be saved all fingerprint information in the encryption domain, so registration accuracy will decline. In addition, it can be seen from Table 4-1, the longer the key length, the system FRR will be higher, because the longer the key, the more we need to reconstruct the real point of a polynomial.

In addition, from **Fig. 9** we can see the order of the polynomial has a certain influence on the system performance, this experiment the key length S is 128 bits, the number of hash points is 200, the experimental test polynomial order n = 7,8,10. The experimental results show that the order of the polynomial is bigger, the higher the system FRR is, this is because with the increasing of polynomial order, the number of required matching fingerprint feature minutiae will increase, thus correctly matching the fingerprint image will be reduced. **Table 4-2** shows the experimental results comparative data

Table 4-2. the impact of polynomial order on the system performance

Polynomial order n	The proposed algorithm		Literature[12] algorithm	
	FRR	FAR	FRR	FAR
n=7	10%	0	9%	0.13%
n=8	11%	0	9%	0.01%
n=10	14%	0	14%	0

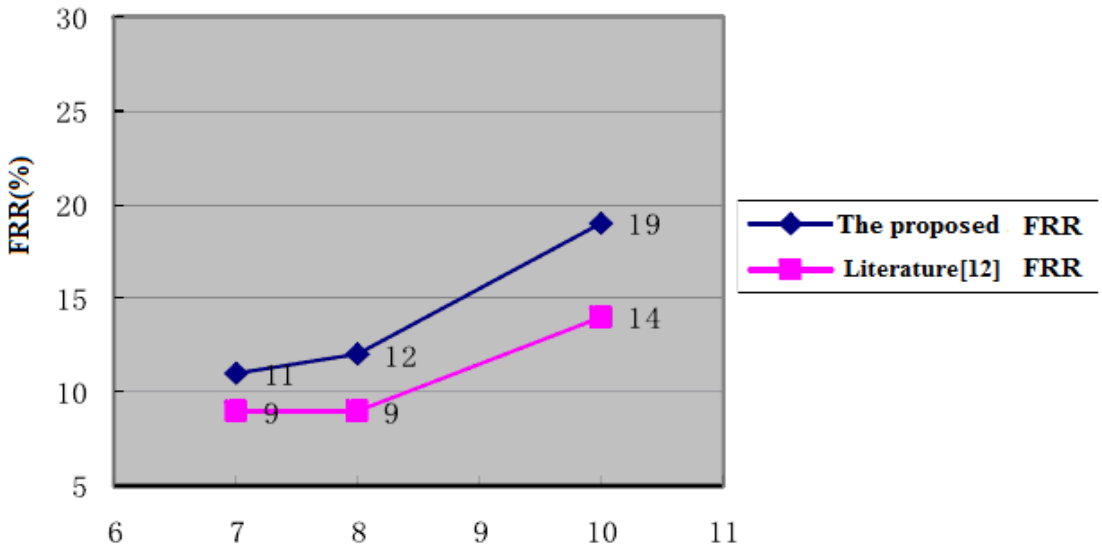


Fig. 9. The impact of polynomial order on the system performance contrast

the number of hash points also cause to impact on system performance, the more hash points, the difficult to find the real point, the harder the key is restored, the system FRR is higher. Since minutia descriptor is used in matching, thus reducing the influence of the number of points hash on system performance. **Table 4-3** shows the minutiae descriptor and the

number of hash points impact on system performance (polynomial order n is 8 bits, the key length is 128 bits)

Table 4-3. minutiae descriptor and the number of hash point's impact on the system performance

Number of Hash points	Using minutia descriptor		Not Using minutia descriptor	
	FRR	FAR	FRR	FAR
150	10%	0	11%	0.01%
200	11%	0	11%	0
250	13%	0	15%	0

5. Conclusions

This paper introduces the Fuzzy Vault algorithm, by combining Fuzzy Vault algorithm with cancelable biometric template, we propose an improved algorithm: firstly we use a special Irreversible function to convert the original fingerprint template into transformation template, and then using the Fuzzy Vault algorithm for protecting keys and transformation template, and combined with minutia descriptor for encrypting the abscissa of the minutiae. The experimental database uses public fingerprint FVC2004 and FVC2002, the result shows that, although the recognition rate of the improved algorithm has a certain drop than the original Fuzzy Vault, but the security performance has been greatly improved, thus the proposed method is feasible in general.

References

[1] Cappelli R., Lumini A., Dario, et al, "Fingerprint Image Reconstruction from Standard Template [J]," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489-1503, 2007. Article (CrossRef Link)

[2] Jain A.K., Nandakumar K., Nagar A., "Biometric Template Security [J]," *EURASIP Journal on Advances in Signal Processing*, Special Issue on Biometrics(1): 1-20, 2008. Article (CrossRef Link)

[3] Yang W, Hu J,Wang S et al., "An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures [J]," *Pattern Recognition*, 47(3):1309-1320, 2014. Article (CrossRef Link)

[4] Nandakumar K., Jain A.K., Pankanti S., "Fingerprint-based Fuzzy Vault: Implementation and Performance[J]," *IEEE Trans. on Information Forensics and Security*, 2(4): 744-757, 2007. Article (CrossRef Link)

[5] Soutar C, Robege D, Stoinov A., "Biometric Encryption: enrollment and verification procedures [C]," *The International Society for Optical Engineering in Optical Pattern Recognition I*, Volume 3386, pp:24-35, 1998. Article (CrossRef Link)

[6] Juels A, "Wattenberg M. A fuzzy commitment scheme[C]," in *Proc. of the 6th ACM conference on Computer and communications security*, New York, USA, Volume 1:28-36, 1999. Article (CrossRef Link)

[7] Hao F., Anderson R., Daugman J., "Combining Crypto with Biometrics Effectively[J]," *IEEE Trans on Computers*, 55(9): 1081-1088, 2006. Article (CrossRef Link)

[8] Jeuls A, Sudan M, "A fuzzy vault scheme[C]," in *Proc. of IEEE International Symposium On Information Theory. Institute of Electrical and Electronics Engineers*, 38(2):237-257, 2002. Article (CrossRef Link)

[9] Clancy T., Kiyavash N., Lin D., "Secure Smartcard-based Fingerprint Authentication[C]," in *Proc.* of WBMA '03 Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, 45-52, 2003. Article (CrossRef Link)
[10] Shenglin Yang, & Verbauwhede,I., "Automatic secure fingerprint verification system based on fuzzy vault scheme[C]," in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing(ICASSP 2005)*,Vol.5:609-612, 2005. Article (CrossRef Link)
[11] Uludag U., Pankanti S., Jain A.K., "Fuzzy Vault for Fingerprint[J]," *Audio and Video-based Biometric Person Authentication*, 92(6): 310-319, 2005. Article (CrossRef Link)
[12] Uludag U, Jain A., "Securing fingerprint template: Fuzzy vault with helper data[C]," in *Proc. of the 2006 Conference on computer Vision and Pattern Recognition Workshop(CVPRW2006)*, New Jersey: IEEE Computer Society, 163, 2006. Article (CrossRef Link)
[13] Nandakumar K., Nagar A, Jain A.K., "Hardening Fingerprint Fuzzy Vault Using Password[C]," in *Proc. of 2nd International Conference on Biometrics, South Korea, Lecture Notes in Computer Science*, 4642,pp: 927-937, 2007.Article (CrossRef Link)
[14] Jesse Hartloff, Sergey Tulyakov, Jimmy Dobler, Atri Rudra, Venu Govindaraju, "Security analysis for fingerprint fuzzy vaults [J]," in *Proc. of SPIE-the International Society for Optical Engineering*, 8712 (4).:1-11, 2013. Article (CrossRef Link)
[15] Li P., Yang X., Cao K, et al., "An Alignment-free Fingerprint Cryptosystem Based on Fuzzy Vault Scheme[J]," *Journal of Network and Computer Applications*, 33 (3): 207-220 , 2010. Article (CrossRef Link)
[16] LI Peng, TIAN Jie, "Biometric Template Protection[J]," *Journal of Software*, *2*0(6): 1553-1573, 2009. Article (CrossRef Link)
[17] ZHANG Rong-lin, LIU Eryun, "Improved cancelable fingerprint fuzzy vault system [J]," *Journal of Xidian University*, 38(4):174-179, 2011. Article (CrossRef Link)
[18] C. Jin and H. Kim, "High-resolution orientation field estimation based on multi-scale Gaussian filter[J]," *IEICE Electronics Express*, 6(24):1781-1787, 2009. Article (CrossRef Link)
[19] L.Hong, Y.Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*,20(8): 777-789, 1998. Article (CrossRef Link)
[20] ORENCIK C., PEDERSEN T.B., SAVAS E., et al., "Securing fuzzy vault schemes through biom etric hashing[J]," *Turk J Elec Eng&Comp Sci*, 18(4): 515-539, 2010. Article (CrossRef Link)
[21] Feng J., "Combining Minutiae Descriptors for Fingerprint Matching[J]," *Pattern Recognition*, 41 (1): 342-352,2008. Article (CrossRef Link)

Feng Wang was born in Anhui Province, China, in 1973. He received B.E. degree and MSc degree from school of computer science and technology at Anhui University of Science & Technology. He is an associate professor with the School of Computer and Information, Fuyang Teachers College, Fuyang, China. His research focuses on image processing and pattern recognition.

Bo Han was born in Anhui Province, China, in 1983. He received the Ph.D. degree from East China Normal University, Shanghai, China in 2012. He is an associate professor with the School of Computer and Information, Fuyang Teachers College, Fuyang, China. His research focuses on designing and modeling of on-chip devices and frequency selective surface.

Lei Niu was born in Anhui Province, China, in 1983. He received the master degree from HeFei University of Technology, HeFei, China in 2008. He is a lecturer with the School of Computer and Information Engineering, Fuyang Teachers College, Fuyang, China. His research focuses on computer network.

Ya Wang received the the Master Degree of Engineering in computer application technology from Guizhou niversity, China,in July 2007.She is currently pursuing a doctoral degree at the College of Electrical and Information Engineering in Anhui University of Science and Technology. She is currently an associate professor with the Department of Science and Engineering ,Fuyang Teachers College,China.Her current research interests include wireless network security and IoT(Internet of things) technology.