ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ՄԱՀԱ ՄԱՀԱԴ ԱԼ ԴԻՆ ՄԱՀԱՄԱԴ ՏՈԼԲԱ

ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԲԱՇԽՎԱԾ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ԿԵՆՍԱՉԱՓՈՂԱԿԱՆ ՊԱՐԱՄԵՏՐԵՐԻ ՀԻՄԱՆ ՎՐԱ

Ե.13.04 - «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ 2011

INSTITUTE OF INFORMATICS AND AUTOMATION PROBLEMS OF NAS RA

MAHA SAAD EL DIN MOHAMED TOLBA

DISTRIBUTED DATA PROTECTION BASED ON BIOMETRIC PARAMETERS

AUTHOR'S ABSTRACT

For obtaining candidate degree in technical sciences in specialty 05.13.04 "Mathematical and software support of computers, complexes, systems and networks"

YEREVAN 2011

Ատենախոսության թեման հաստատվել է Հայաստանի Պետական Ճարտարագիտական Համալսարանում (Պոլիտեխնիկ)

Գիտական ղեկավար՝	տ.գ.թ., դոցենտ	Գ. Ի. Մարգարով
Պաշտոնական ընդդիմախոսներ՝	ՀՀ ԳԱԱ ակադ., տ.գ.դ., պրոֆ.	Գ. Հ. Խաչատրյան
	տ.գ.թ., դոց.	Ռ. Գ. Հակոբյան

Առաջատար կազմակերպություն՝ Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ

Պաշտպանությունը կայանալու է՝ 2011թ. հոկտեմբերի 27-ին, ժ. 15^{00}-ին, 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացված պրոբլեմների ինստիտուտում (հասցեն՝ 0014, Երևան, Պ. Սևակ փ. 1)

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2011թ. սեպտեմբերի 26-ին.

037 Մասնագիտական խորհրդի գիտական
քարտուղար, ֆ.-մ.գ. դ., պրոֆ Մ.Ե. Հարությունյան

The subject of the dissertation has been approved in State Engineering University of Armenia (Polytechnic).

Scientific Advisor:	Cand. of Tech. Sc.	G. I. Margarov
Official opponents:	Acad. of NASRA, Dr. of Tech. Sc., Prof.	G. H. Khachaturyan
	Cand. of Tech. Sc.	R.G. Hakobyan

Leading organization: Yerevan Telecommunication Research Institute

The defense will take place on 27th of October 2011, at 15^{00} in the Institute of Informatics and Automation Problems of NAS RA, during the session of the 037 “Informatics and computer systems” special council (address: 1 P. Sevak str. 0014, Yerevan).

The dissertation is available at the library of the institute.
Author’s abstract is sent on 26th of September 2011

Scientific secretary of the specialized council 037:
Dr. of Phys. and Math. Sc., Prof. M. E. Haroutunian

CHARACTERIZATION OF THE THESIS

Actuality of the subject. As our everyday life is getting more and more computerized, automated security systems are getting more and more important. For example, today most of the banking transactions can be performed over the internet. This rapid progress in wireless communication system, personal communication system and smart card technology in our society makes information more susceptible to abuse. Due to the growing importance of the information technology, the necessity of data protection and access restriction, it is necessary to have a reliable personal authentication.

In today's advanced digital technology world, there is an increased requirement of security measures leading to the development of many based personal authentication systems. The key task of an authenticated system is to verify that the users are in fact who they claim to be. There are three main methodologies which can perform this verification; the security system could ask the user to provide some information known only to the user, it could ask the user to provide something only the user has access to or it could identify some sort of trait that is unique for the user. Identifying some trait that is unique for the user is known as biometric security. A biometric system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user. Fingerprints are the most widely used parameter amongst all biometrics. The reason behind the popularity of fingerprint-based recognition among the biometrics-based security systems is the un-changeability of fingerprints during the human life span and their uniqueness.

From the discussion above, the aim of this research is to investigate the feasibility of constructing a biometric authentication system where the biometric template is protected at the time of storage and at the time of matching. Most existing biometric authentication systems store their template securely using an encryption function. However, in order to perform matching, the enrolled template must be decrypted. It is at this point that the authentication system is most vulnerable as the entire enrolled template is exposed. A biometric is irreplaceable if compromised. It can also reveal sensitive information about an individual. If biometric systems are taken up widely, the template could also be used as an individual's digital identifier. Compromise in that case, violates an individual's right to privacy as their transactions in all systems where they used that compromised biometric can be tracked. This thesis studies a cryptographic construct developed from error tolerant cryptography for secure comparison of templates, the Fuzzy Vault system. Minutiae-based template extraction algorithm is represented so that they can be incorporated into these cryptographic constructs.

The problem of data protection is one of the various types of security problems. Data protection arises from the need to store important information from getting lost, destroyed or into wrong hands. The modern approach to the solution of this problem suggests combining cryptography and biometrics. The merging between both of them has led to the development of cryptographic constructs where the secret data is protected using the biometric characteristics. One of the cryptographic constructs is the fingerprint fuzzy vault scheme. This construct has some security drawbacks. The locations of the points in the vault may reveal some information as to which points are genuine depending on the chaff point generation method. Another drawback is that construct is vulnerable to brute force attack.

Objectives of the work are. The main purpose and objective of the work is to research and develop the principles for increasing the performance and secrecy of the fingerprint fuzzy vault scheme used for secret data protection. Because the scheme depends on fingerprints, another objective is to develop minutiae extraction system with high quality.

To achieve this goal it is necessary to solve the following tasks:

- Analyze the fingerprint image quality and identify methods to improve the performance of the fingerprint enhancement process.
- Design and develop a fingerprint minutiae extraction model to extract true minutiae points in terms of their locations from the enhanced image to increase the performance of the fuzzy vault construct.
- To research and develop methods to overcome the fuzzy vault construct drawbacks and weakness.
- Construct new algorithms and corresponding software tools which will utilize the fingerprint fuzzy vault scheme on basis of the developed methods.

Objects of the research. Objects of the research are the constructs that enable protection and secure storage of secret data for authentication applications.

Methods of research. Studies conducted in the work, based on the integrated use of methods of cryptography, biometrics, image processing, mathematical analysis, combinatorial analysis and the theory of algorithms.

Scientific novelty

- A method for fingerprint image enhancement has been developed which increases the quality measurements of the minutiae extraction process.
- A minutiae extraction model has been presented and evaluated using two quality measurements namely sensitivity and specificity. The high values of sensitivity and specificity refer to the effectiveness of the model. They indicate the ability of the presented model to detect the true minutiae and remove the false minutiae for fingerprint image.
- A method for fingerprint fuzzy vault construct with high level of secrecy has been developed, which in comparison with the existing one decreases the success rate of brute force attack.

Practical significance

- The software modules have been developed intended for fingerprint image enhancement and minutiae extraction system that can be used in different applications for fingerprint recognition.
- The software is developed for research works that supports effective research and analysis for fingerprint FuzzyVault system using automated fingerprint minutiae extraction system.
- The fingerprint fuzzy vault system is designed that provides a secure data protection that increases the number of operations needed to break the system by almost 30 times.

Practical implementation. Results of the thesis are used at information security and software development department in State Engineering University of Armenia (SEUA) by means of FuzzyVault software tool. This software is used as an alternative way to secure application data in scientific researches.

The following topics are presented to the defense

- The approach for fingerprint image enhancement and minutiae extraction and validation from the enhanced fingerprint image.
- The approach for chaff points generation and distribution for fingerprint fuzzy vault cryptographic construct.
- The software for FuzzyVault tool for protection and secrecy of a secret data using the fingerprint fuzzy vault cryptographic construct.

Approbation of thesis. The main results of the thesis have been presented and discussed at:

- The Annual Conference of SEUA, Yerevan, 2009.
- International conference "Computer Science and Information Technologies (CSIT)" (Yerevan, Armenia) in 2009.
- Series of international conferences "Security and Management" at WorldComp. (Las Vegas, USA) in (2009, 2010).
- International Workshop in Applications of Information Theory, Security and Coding, at (Institute of Informatics and Automation Problems of National Academy of Sciences of the Republic of Armenia) , April 2010.
- XXXV International Youth Scientific conference "Gagarin readings" (MATI, Moscow, Russian), in 2010.
- International Scientific – Practical Conference "Safety Issues for Information systems" at Armenian Technological Academy, (Yerevan, Armenia), in 2011.
- Scientific seminars at SEUA, in (2009, 2011) and a scientific seminar at IIPA NAS, 2011.

Publications. Eight scientific articles are published on the materials and results of the thesis; the list is presented at the end of the abstract.

The structure and volume of the work. The dissertation consists of an introduction, four chapters, conclusion, the list of references with 76 entries and two appendices. The total volume of the dissertation is 141 pages, with 6 tables and 62 figures. The thesis is written in English.

CONTENTS OF RESEARCH

Introduction , which describes the actuality of the subject, objectives of the work, scientific novelty and practical significance of the work as well as gives the information about the practical implementation of the results.

Chapter 1 is dedicated to an overview of biometrics especially fingerprints and how it can be used for data protection using biometric cryptographic construct called fuzzy vault scheme. It consists of 5 sections.

Section 1.1 gives an overview about different types of biometrics, requirements of biometric identifiers, biometric technologies, biometric operational mode, biometric system performance and biometric systems applications.

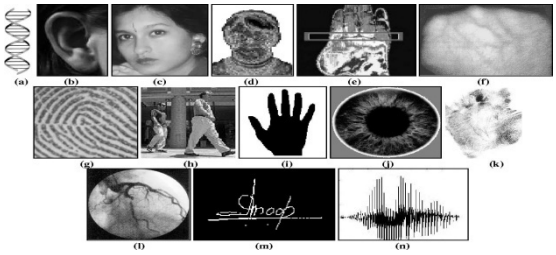


Fig. 1. Examples of biometric characteristics

Section 1.2 represents an analysis for the fingerprint image in terms of fingerprint representation area, fingerprint pattern analysis, main modules for fingerprint recognition system, and different types of fingerprint sensors. Fingerprint-based system is the oldest method of all the biometrics techniques being used today, which has been successfully used in numerous applications. Every one is known to possess a unique fingerprint and it does not change throughout his lifetime. A fingerprint is a unique pattern of ridges and valleys on the surface of finger of an individual. A ridge is defined as single curved segment, and a valley is the region between two adjacent ridges. There are two types of fingerprint representations: global and local. Global representations of the fingerprint based on cores and deltas. Local representations predominantly based on ridge endings or bifurcations (known as minutiae) as shown in fig. 2. Sir Francis Galton (1822-1922) was the first person who observed the structures and permanence of minutiae. Therefore, minutiae are also called "Galton details". Minutiae are the most common, primarily due to the following reasons:

- Minutiae capture much of the individual information.
- Minutiae-based representations are storage efficient.
- Minutiae detection is relatively robust to various sources of fingerprint degradation.

Typically, minutiae-based representations rely on locations of the minutiae and the directions of the ridges at the minutiae location.

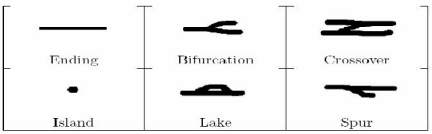


Fig. 2. Common minutiae types.

In **section 1.3,** the secret sharing schemes and definitions are considered.

Section 1.4 presents the concept of biometric cryptographic constructs. Fuzzy vault construct is an example of biometric cryptographic constructs which aims to secure critical data with fingerprint parameters in a way that only the authorized user can access the secret data by providing the valid fingerprint.

Summary of chapter 1 is given in **section 1.5.**

Chapter 2 describes a proposed fingerprint image enhancement approach. The performance of a fingerprint feature extraction algorithm depends critically upon the quality of the input fingerprint image. Poor quality fingerprints lead to the generation of spurious minutiae. In smudgy regions, genuine minutiae may also be lost, the net effect of both leading to loss in accuracy of the extractor. The robustness of the recognition system can be improved by incorporating an enhancement stage prior to feature extraction. This chapter consists of 3 sections.

In section 2.1 and its subsections, we present the proposed algorithm for fingerprint image enhancement based on image segmentation. The proposed algorithm is able to successfully segment the fingerprint images.

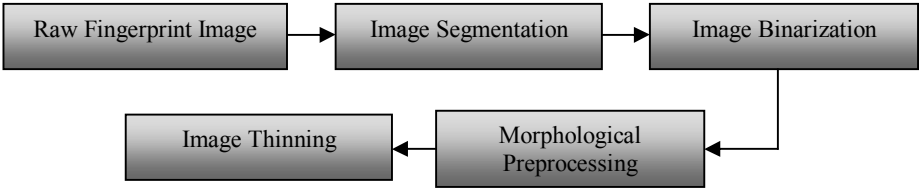


Fig. 3. The proposed enhancement processes.

In subsection 2.1.1, an image segmentation process is used for separating the foreground regions in the image from the background regions. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the region of interest (ROI). The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information. When minutiae extraction algorithms are applied to the background regions of an image, it results in the extraction of noisy and false minutiae. In a fingerprint image, the background regions generally exhibit a very low grey-scale variance value, whereas the foreground regions have a very high variance. Hence, a method based on variance threshold can be used to perform the segmentation. Firstly, the image is divided into blocks and the grey-scale variance is calculated for each block in the image. If the variance is less than the global threshold, then the block is assigned to be a background region; otherwise, it is assigned to be part of the foreground. The grey-level variance for a block of size $W \times W$ is defined as:

$$V(k) = \frac{1}{W^2} \sum_{\substack{0 \le i \le W-1 \\ 0 \le j \le W-1}} (I(i,j) - M(k))^2 \quad (1)$$

Where: $V(k)$ is the variance for block k, $I(i, j)$ is the grey-level value at pixel (i, j), $M(k)$ is the mean grey-level value for the block k.

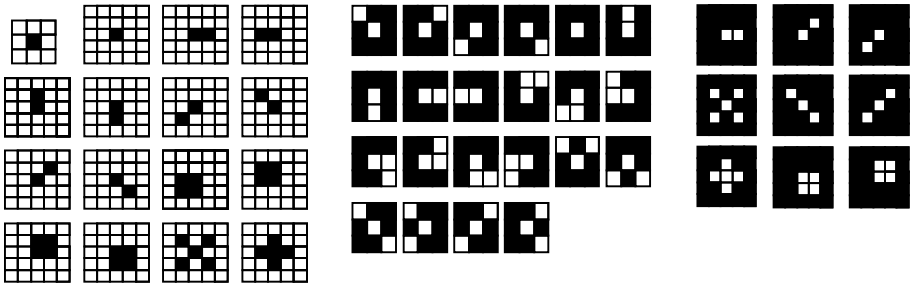
In subsection 2.1.2, image adaptive binarization is used to convert a 256 grey level image to a binary image. The simplest way to use image binarization is to choose a threshold value, and classify all pixels with values above this threshold as white, and all other pixels as black. In binarization approach, the grey scale image is converted into a binary image prior to minutiae detection. The straight forward approach for binarization relies on choosing a global threshold $T=V_{mean}$. The binarization is then done according to the following equation:

$$V_{mean} = \frac{1}{W^2} \sum_{\substack{0 \le i \le w-1 \\ 0 \le j \le w-1}} V(i,j) \quad (2)$$

In our proposed algorithm, adaptive image binarization is used where an optimal threshold is chosen for each image block w×w using equation (2).

In subsection 2.1.3, After close examination of the binarized image, the misconnections and isolated regions (dots, holes, islands, etc.) in a binary image may introduce a number of spurious minutiae in thinned images. Therefore some morphological operators are applied to the binarized image. In this section, image noise elimination is described where unwanted noise is removed by using 5*5 structuring elements then by using 3*3 structuring elements represented in fig.4(a).

In subsection 2.1.4, image smoothing is applied to the fingerprint image where all holes in the image will be filled up by using 5*5 structuring elements then by using 3*3 structuring elements represented in fig.4 (b, c).



(a) (b) (c)

Fig. 4. (a) 3*3 and 5*5 structuring elements used in noise elimination. (b) 3*3 structuring elements used in smoothing stage. (c) 5*5 structuring elements used in smoothing stage.

In subsection 2.1.5, the fingerprint image is thinned to one pixel wide, but the algorithm had to be modified to apply to fingerprint ridge thinning. The problem lies in what is defined to be a one-pixel width skeleton. In the case of fingerprint ridges a ridge point that is not minutiae is only allowed to have two neighbors that belong to the ridge. This fact conflicts with the second condition in the original thinning algorithm. The problem arises in 16 special cases where not all neighbor pixels, which belong to the background, are connected but where the pixel still should be deleted. Sixteen structuring elements of twenty eight structuring elements used are shown in fig.5.

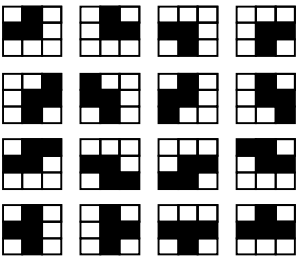


Fig. 5. Examples of structuring elements used in modified thinning process.

Section 2.2 is dedicated to results and analysis of the proposed system. The original image that is loaded into the system is a *256* gray-scale bitmap image with 128 x 128 pixels size as shown in fig.6 (a). There are five processes in image processing stage. Output of each process will be fed into the next step for further purpose. The result for each process in image processing stage is shown in

fig.6. The output of the image segmentation process is shown in fig.6 (b). The result shows that the output image has been cropped and only depicts the fingerprint. The noise in the background has been deleted. The output of the adaptive binarization process is shown in fig.6 (c). The result shows that the gray-scale image has been converted to black and white image. The small dots that exist in the binary image are noise due to poor fingerprint acquisition. The noise has been removed after going through the noise elimination module, as shown in fig.6 (d). Fig.6 (e) shows the result of smoothing module where holes that existed in the image have been filled. The image is thinned to one-pixel width after fed through thinning module as shown in fig.6 (f). These results show that each module has performed its task as expected. Summary of chapter 2 is given in **section 2.3.**

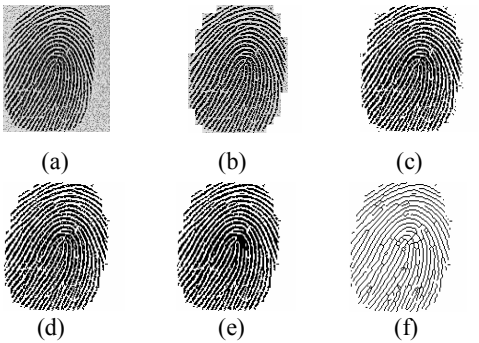


Fig. 6. The output of different stages of the proposed enhancement algorithm.

In chapter 3, after the fingerprint image has been enhanced and thinned; it will be fed to the feature extraction stage as shown in fig. 7. The goal of this stage is to extract the minutiae point from the thinned image. Following the extraction is minutiae validation process that eliminates the false minutiae before using the template for locking/ unlocking the fuzzy vault scheme. This chapter consists of 4 sections.

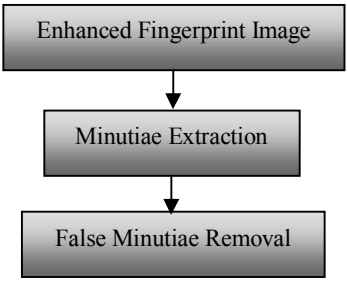


Fig. 7. The proposed feature extraction algorithm.

In section 3.1, both minutiae types are extracted using the crossing number method according to the following equation.

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| \qquad P_9 = P_1 \tag{3}$$

The minutiae type can be either ridge ending or ridge bifurcation.

- If CN = 1, the pixel is declared as ridge ending point and its x and y coordinates are recorded.
- If CN = 3, the pixel p is declared as bifurcation point and its x and y coordinates are recorded.

In section 3.2, the minutiae points extracted in minutiae extraction step may contain false minutiae points due to noisy image or artifacts created by the thinning process. A validation algorithm is used to validate the minutiae points extracted from the extraction algorithm. The proposed algorithm operates on the skeleton image. This approach incorporates the validation of different minutiae into a single algorithm. It tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the minutiae. The algorithm is able to cancel out false minutiae based on the configuration of the ridge pixels connected to the minutiae point.

For each candidate minutiae (ridge ending or ridge bifurcation):

- Create and initialize with 0 an image L of size W x W. Each pixel of L corresponds to a pixel of the thinned image which is located in a W x W neighborhood centered in the candidate minutiae.
- Label with -1 the central pixel of L. This is the pixel corresponding to the candidate minutiae point in the thinned ridge map image.
- If the candidate minutiae is a ridge ending then:
  (a) Label with 1 all the pixels in L which correspond to pixels connected with the candidate ridge ending in the thinned ridge map image.
  (b) Count the number of 0 to 1 transitions (T_{01}) met when making a full clockwise trip along the border of the L image.
  (c) If $T_{01} = 1$, then validate the candidate minutiae as a true ridge ending.
- If the candidate minutiae is a ridge bifurcation then:
  (a) Make a full clockwise trip along the 8 neighborhood pixels of the candidate ridge bifurcation, and label in L with 1, 2 and 3 respectively the three connected components met during this trip.
  (b) For each L = 1,2,3, label with L all pixels in L which:
    i. Have the label 0;
    ii. Are connected with an L labeled pixel;
    iii. Correspond to 1 valued pixels in the thinned.
  (c) Count the number of 0 to 1, 0 to 2 and 0 to 3 transitions met when making a full clockwise trip along the border of the L image. The above three numbers are denoted by T_{01}. T_{02} and T_{03} respectively.
  (d) If $T_{01} = 1$ and $T_{02} = 1$ and $T_{03} = 1$, then validate the candidate minutia as a true ridge bifurcation.

The dimension W of the neighborhood analyzed around each candidate minutiae is chosen larger then two times the average distance between two neighborhood ridges. In this way the algorithm succeeds to cancel close minutiae belonging to the same ridge. In our model W x W equals (15 x 15).

In section 3.3, we have tested the proposed algorithm using two quality measurements namely sensitivity and specificity defined by equations 4, 5 which indicate the ability of the proposed algorithm to detect the genuine minutiae and remove the false minutiae for fingerprint image. The high values of sensitivity and specificity suggest the effectiveness of the proposed algorithm.

$$\text{Sensitivity} = 1 - \frac{\text{Missed Minutiae}}{\text{Ground Truth Minutiae}} \tag{4}$$

$$\text{Specificity} = 1 - \frac{\text{False Minutiae}}{\text{Ground Truth Minutiae}} \quad (5)$$

The sensitivity and specificity of the proposed algorithm are evaluated for example images and results are shown in table 1.

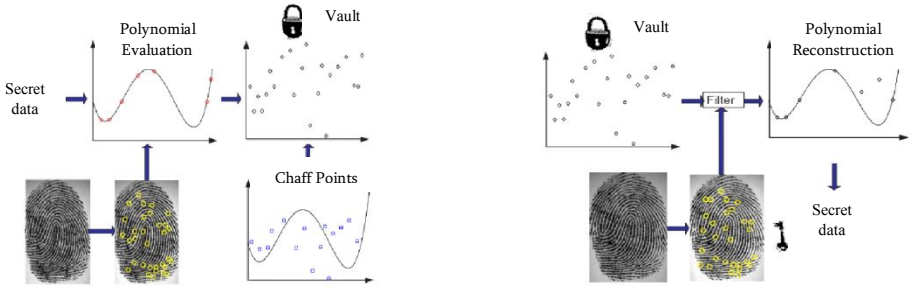
Table 1. Total, missed and false number of minutiae after post processing with the sensitivity and specificity of the proposed technique.

Image	Ground Truth Minutiae	Post processed			Sensitivity %	Specificity %
		Total	Missed	False		
I1	59	62	1	4	98.3%	93.2%
I2	56	58	2	4	96.4%	92.8%
I3	40	39	1	0	95%	100%
I4	36	37	1	2	97.2%	94.4%

Summary of chapter 3 is given in **Section 3.4.**

In chapter 4, In this chapter, a fully automatic and implementation of the fuzzy vault scheme using fingerprints is demonstrated even though our implementations are relatively straightforward extensions of the implementation by Uludag et al. , the issues for chaff points generation and distribution in implementing the fuzzy vault are non- trivial.

In section 4.1 Fuzzy vault anatomy is explained. The fuzzy vault scheme is governed by two basic operations namely *locking* and *unlocking*. All the steps required to lock a secret in the Fuzzy Vault are graphically represented in fig.8.



(a)Vault locking (b) Vault unlocking

Fig. 8. Fingerprint fuzzy vault scheme.

In section 4.2 The fuzzy vault scheme based on biometrics enables privacy for data protection. The fuzzy vault allows for some minor differences between the unordered sets used to lock and unlock the vault. This fuzziness is necessary for use with biometrics, since different measurements of the same biometric often result in quite different signals, due to a noise in the measurement or non-linear distortions.

In section 4.3 The fuzzy vault scheme using fingerprints by Uludag et al. is demonstrated. To bypass the problem of matching the minutiae points and finding an upper bound for the performance of the scheme, the author has used a fingerprint database where minutiae points and the correspondence between template and query fingerprints were established manually by an expert. Also we analyze some security drawbacks of the fuzzy vault scheme as outlined below:

- The locations of the points in the vault may reveal some information as to which points are genuine depending on the chaff point generation.
- Mihailescu pointed out that the fuzzy vault scheme is vulnerable to brute force attack.

In section 4.4, the proposed fingerprint fuzzy vault scheme with modifications to overcome the drawbacks of the existing system is explained.

In section 4.4.1, the locking portion of the system is described for the creation of the fuzzy vault for the secret data to be protected. A template created from the fingerprint image (in terms of minutiae coordinates) is used as vault true data points to encode the secret data defined by the coefficients of a polynomial defined by the following equation.

$$f(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ \ldots + a_{M-1} \cdot x^{M-1} = \sum_{i=0}^{M-1} a_i \cdot x^i \qquad (6)$$

Data points that represent the polynomial are stored in the fuzzy vault. Many random data points (chaff) are added to the vault to hide the identity of the true polynomial data points. The proposed algorithm in chapter 3 is used to create the fingerprint template. The fuzzy fingerprint vault Locking block diagram is shown in fig.9.

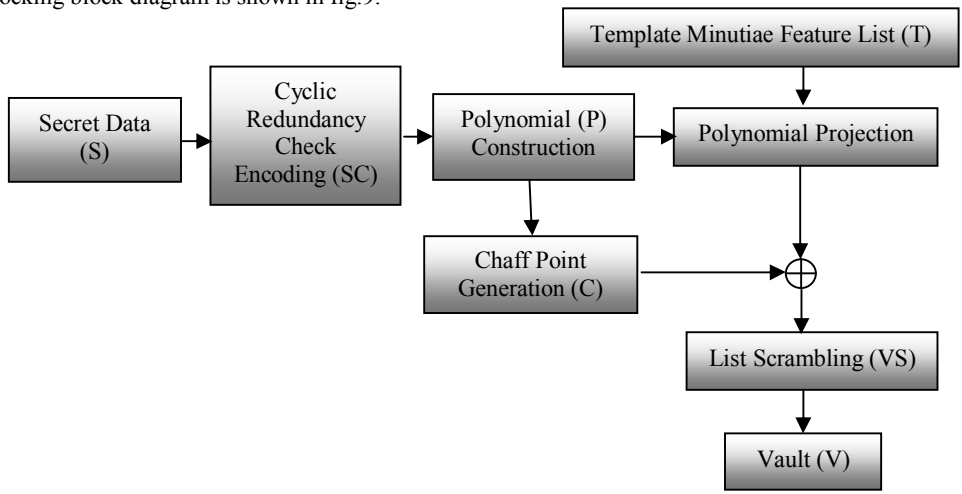


Fig. 9. Fingerprint fuzzy vault locking.

The analysis shows that the minimum distances between any chaff points and any genuine points is an important parameter, which affects the performance of the scheme. When we randomly generate the chaff points, we need to make sure the minimum distance is satisfied. The minimum distance needs to be at least twice as large as the acceptable distance of a minutia position between different scans. Figure 10 shows the relationship between the minimum distance and the matching accuracy. Besides the minimum distance, the number of the chaff points also needs to be taken into consideration during the fuzzy vault constructing. If the number of the chaff points is set too small, according to the unlocking algorithm, the chaff points are more likely to be closer to the genuine points, which will result in higher false accept rate (FAR). Similarly, if the size of chaff points is too

big, a genuine point is more likely to be classified as a chaff point. This will lead to higher false reject rate (FRR).

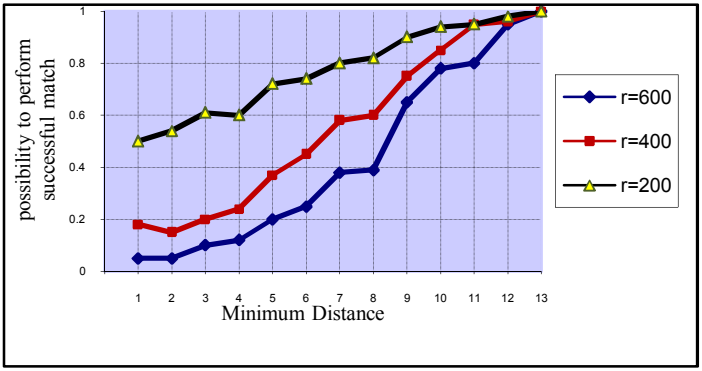


Fig. 10. The possibility of successful matching and the minimum distance of chaff point for different chaff sizes.

In subsection 4.4.2, we explain two proposed modifications to the chaff points generation and distribution stage in order to strengthen the fuzzy vault against possible attacks. We generate the chaff points with the condition that every chaff point in the vault should be at least t Euclidean distance apart from a genuine point and should be at least t' Euclidean distance apart from any other chaff point. Note that $t' < t$ since having chaff points far from the genuine points are desirable and have a positive effect on false reject rate (FRR). Smaller threshold t', on the other hand, for inter-chaff point distance is necessary to imitate the distribution of genuine points where close genuine points occasionally occur in the vault. While t value depends on the fingerprint image size and the total number of points in the vault, t' should be chosen depending on the distribution of genuine points. Our proposed method to improve the security involves the idea that, by choosing the chaff points at random, but in a more clever way, we can embed some other (randomly chosen) polynomials of degree $k-1$ other than the secret polynomial in the vault. If we guarantee that the number of chaff points that lie on these (chaff) polynomials, is around n - the same number of genuine points on the secret polynomial on average - the attacker cannot distinguish the secret polynomial from the fake ones. Otherwise the attacker who succeeds to construct a polynomial can discard it if there are fewer points. With the proposed chaff generation method, we allow each polynomial intersect with other polynomials in at least k vault points which increases the maximum number of polynomials we can embed into the vault. Note that any two polynomials cannot intersect with each other in more than $k-1$ points. As a result of our experiments in our setting described above, we are able to hide around 30 chaff polynomials in the vault. Therefore, this method decreases the probability of finding the secret polynomial using Mihailescu's attack from 100% to less than 4% after the brute force attack is applied.

In subsection 4.4.3, revealing the secret data using polynomial reconstruction is discussed. To reconstruct the secret data polynomial, Lagrange interpolation method is used as defined by the following equation.

$$L_n(x) = \sum_{i=0}^{N-1} y_i \prod_{i \neq k} \frac{x - x_k}{x_i - x_k} \tag{7}$$

The user must identify true values from the vault, since the corresponding (X, Y) pairs define the polynomial. The X' data is used to select the true values from the vault. Since biometric data are

expected to be inexact (due to acquisition characteristics, sensor noise, etc.), X' template values are matched to X vault values within a predefined threshold distance (quantization), thus allowing for exact matching. This is the "fuzziness" built into the system, since multiple X' values (i.e., those within the threshold distance of X values) will result in a single X value. Fig.11 represents block diagram for fingerprint fuzzy vault unlocking.

In the case of the fingerprint fuzzy vault of polynomial degree 8, chaff points 300, genuine points 30, if the adversary uses brute force attack, the attacker has to try a total of (330, 9) combination of 9 elements each. Only (30, 9) of these combinations are required to decode the vault. Hence for an attacker to decode the vault it takes Combination of (330, 9) / Combination (30, 9) evaluations.

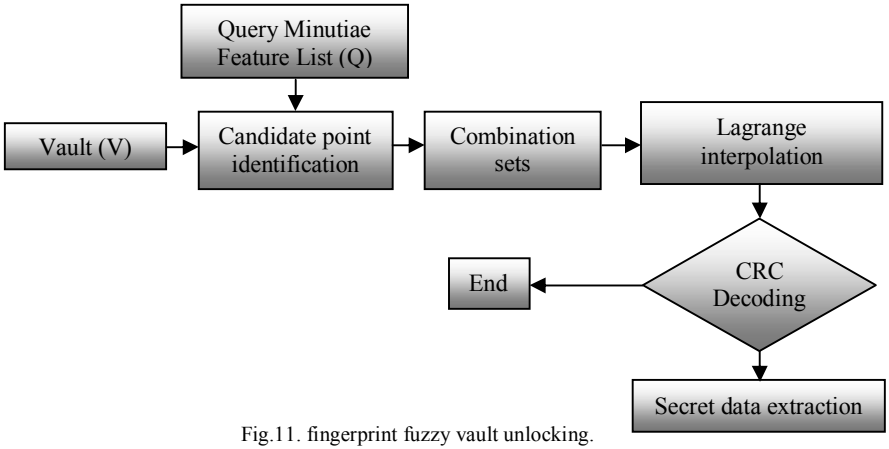


Fig.11. fingerprint fuzzy vault unlocking.

Section 4.5 is dedicated to r*esults and analysis.* For security analysis Maihailescu provides a strong brute force attack which finds the secret polynomial in less than:

$$\text{No. of operations} = 8.(c.k).(c/n)^k \quad (8)$$

Where c: no. of chaff points in the vault, n: no. of genuine points in the vault, k: no. of points needed to reconstruct polynomial of degree (k-1). For our proposed system: C=300, n= 30, k=9. By substituting in equation (8), breaking the system requires: $8*300*9*[(300/30)^9] \approx 2*10^{13}$ operations. As a result of our experiments in our setting described above, we are able to hide around 30 chaff polynomials in the vault. Therefore, this method decreases the success rate of finding the secret polynomial using Mihailescu's attack from 100% to less than 4 % after the brute force attack is applied. Table 2 presents a comparison between Uldage FFV scheme and the proposed FuzzyVault scheme.

Table 2. Comparison between Uldage FFV and the FuzzyVault

Method	Minutiae Extraction Method	The Success Rate of Brute Force Attack
Uludag FFV Scheme	Manually by an expert	100%
FuzzyVault Scheme	Automatically	< 4%

In section 4.6, Program realization for the proposed fingerprint fuzzy vault scheme has been developed. The software for all algorithms and graphical user interface (GUI) has been developed using Microsoft Visual Studio 2010 (C# programming language) on a Laptop HP Compaq with Genuine Intel core2 duo CPU T2250 @1.73GHz, 1.49GB of RAM.
Summary of chapter 4 is given in **section 4.7.**

Main results of the dissertation

1. A method for fingerprint image enhancement has been developed which increases the quality measurements of the minutiae extraction process.
2. A minutiae extraction model has been presented and evaluated using two quality measurements namely sensitivity and specificity. The high values of sensitivity and specificity refer to the effectiveness of the model. They indicate the ability of the proposed model to detect the true minutiae and remove the false minutiae for fingerprint image.
3. A novel approach to fingerprint fuzzy vault construct with high level of secrecy has been developed, which in comparison with the existing fingerprint fuzzy vault scheme decreases the success rate of brute force attack.
4. The software modules have been developed intended for fingerprint image enhancement and minutiae extraction system that can be used in different applications for fingerprint recognition.
5. The software is developed for research works that supports effective research and analysis for fingerprint FuzzyVault system using automated fingerprint minutiae extraction system.
6. The fingerprint fuzzy vault system is designed that provides a secure data protection that increases the number of operations needed to break the system by almost 30 times.

LIST OF PUBLICATIONS ON THE TOPIC OF THE THESIS

[1] M. Tolba, Actual problems of information security based on biometrics // Proceedings of the State Engineering University of Armenia (*Polytechnic*)-Yerevan, 2009. Part 1, No. 1, pp. 428-432.

[2] G. Margarov, M. Tolba, Biometrics based secret sharing using fuzzy vault // Proceedings of the 7th International Conference "Computer Science and Information Technologies", CSIT'09, Yerevan, Armenia, 2009, pp. 177-180.

[3] G. Margarov, M. Tolba, Fingerprint biometric solution for securely secret sharing // Proceedings of the 2009 International Conference on Security & Management, SAM'09, July 13-16 Las Vegas, USA, 2009, CSREA Press, pp. 211-213.

[4] M. Tolba, T. Andreasyan, An algorithm for computing fingerprint minutia points // XXXV International Youth Scientific conference "Gagarin readings", MATI, Moscow, 2010, vol. 4 – pp. 58 –60 (in Russian).

[5] M. Tolba, E. Hovhannisyan, On pro-active secret sharing schemes // XXXV International Youth Scientific conference "Gagarin readings", MATI, Moscow, 2010, vol. 4 – pp. 55 – 56.

[6] G. Margarov, M. Tolba, Share renewal protocol in the presence of active attackers // Proceedings of the Workshop on Applications of Information Theory, (WAITSC2010), Coding and Security, April 14-16, Yerevan, Armenia, 2010, pp. 59-62.

[7] M. Tolba, V. Markarov, T. Andreasyan, A New approach for fingerprint minutia extraction algorithm // Proceedings of the 2010 International Conference on Security & Management, SAM'10, July 12-15 Las Vegas, USA, 2010, CSREA Press, pp. 577-583.

[8] M. Tolba, "An improved fuzzy vault scheme", In Proceedings of the 2011 International Scientific-Practical Conference "Safety Issues for Information Systems", May 26-27 at Armenian Technological Academy, Yerevan, Armenia, 2011, pp. 78-82.

Մահա Սաադ Էլղին Մոհամեդ Տոլբա

ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԲԱՇԽՎԱԾ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ԿԵՆՍԱՉԱՓՈՂԱԿԱՆ ՊԱՐԱՄԵՏՐԵՐԻ ՀԻՄԱՆ ՎՐԱ

ԱՄՓՈՓԱԳԻՐ

Քանի որ մեր առօրյան դառնում է ավելի քոմփյութերացված, անվտանգության ավտոմատացված համակարգերը դառնում են ավելի պահանջված: Օրինակ՝ այսօր բանկային հիմնական գործառույթները կատարվում են ինտերնետի միջոցով: Տեղեկատվական տեխնոլոգիաների և տվյալների պաշտպանության անհրաժեշտության կարևորության աճի հետ մեկտեղ, անհրաժեշտ է ապահովել վստահելի անվտանգության համակարգի առկայությունը:

Ներկա զարգացած թվային տեխնոլոգիաների աշխարհում անհրաժեշտ է առավել բարձր անվտանգության միջոցներ, ինչը բերում է անհատական վավերականացման համակարգերի մշակման: Վավերականացման համակարգերի հիմնական նպատակն է ստուգել օգտագործողի իսկությունը: Գոյություն ունի ստուգման երեք հիմնական եղանակ: Անվտանգության համակարգը կարող է օգտագործողից կատարել որոշակի տեղեկությունների հարցում, որը հայտնի է միայն իրեն, կարող է հարցնել որևէ բան, ինչը միայն օգտագործողին է հասանելի, կամ կարող է ճանաչել որևէ բնութագիր, որը յուրահատուկ է օգտագործողի համար: Օգտագործողի որոշակի յուրահատկության կիրառումը նույնականացման գործընթացում հայտնի է որպես կենսաչափողականություն: Կենսաչափողական համակարգն իրենից ներկայացնում է ճանաչողական համակարգ, որն օգտագործողի ֆիզիոլոգիական կամ վարքագծային բնութագրի հիման վրա իրականացնում է վավերականացում: Մատնահետքը ամենատարածված կենսաչափողական բնութագիրն է և նրա վրա հիմնված կենսաչափողական անվտանգության համակարգի տարածվածության պատճառն է նրա յուրահատկությունը և անփոփոխությունը մարդու ամբողջ կյանքի ընթացքում:

Տվյալների պաշտպանության խնդիրը տեղեկատվական անվտանգության տարատեսակ խնդիրներից մեկն է: Տվյալների պաշտպանության պահանջը պայմանավորված է կարևոր տեղեկությունը կորստից, վնասումից կամ ոչ իրավասու անձանց տիրապետումից պաշտպանելու անհրաժեշտությամբ: Վերոնշյալ խնդրի լուծման ժամանակակից մոտեցումը ենթադրում է գաղտնագրության և կենսաչափողական սկզբունքների միավորում: Այս միավորման դեպքում գաղտնի տվյալների պաշտպանությունը կատարվում է կենսաչափողական հատկանիշների հիման վրա, որը կարող է ապահովել ավելի բարձր անվտանգության մակարդակ: Պաշտպանվածության լրացուցիչ մակարդակ կարող է ապահովել նաև գաղտնագրված տեղեկությունների ոչ հստակ պահոցում թաքցնելը: Այս կառուցվածքն ունի որոշակի թերություններ: Կետերի տեղաբաշխումը պահոցում կարող է որոշակի տեղեկություն բացահայտել իրական կետերի մասին, կեղծ կետերի ներքո: Մեկ այլ թերություն է կառուցվածքի խոցելիությունը հատարկման հարձակումներից:

Հետազոտության հիմնական նպատակը

Աշխատանքի հիմնական նպատակը և խնդիրն է հետազոտել և մշակել մատնահետքերի համար ոչ հստակ պահոցի սխեմայի գաղտնիության և արդյունավետության բարձրացման սկզբունքները: Քանի որ մեթոդը հիմնված է մատնահետքի վրա, ապա ևս մեկ նպատակ է մշակել մատնահետքից հատուկ կետերի առանձնացման բարձրորակ համակարգ:

Նշված նպատակին հասնելու համար աշխատանքում լուծվել են հետևյալ խնդիրները՝

1. Հետազոտել մատնահետքերի պատկերի որակը, և բացահայտել լավարկման գործընթացի արդյունավետությունը բարելավելու մեթոդներ:
2. Նախագծել և մշակել մատնահետքերից հատուկ կետերի առանձնացման մոդել, որը հնարավորություն է տալիս մատնահետքի լավարկված պատկերից ստանալ իրական հատուկ կետերի տեղաբաշխումը, ոչ հստակ պահոցի կառուցվածքի արտադրողականության բարձրացման նպատակով:
3. Հետազոտել և մշակել ոչ հստակ պահոցի կառուցվածքի թերությունների և թուլությունների հաղթահարման մեթոդներ:
4. Մշակել նոր ալգորիթմ և համապատասխան ծրագրային միջոցներ, որոնք կիրագործեն մատնահետքի հիման վրա ոչ հստակ պահոցի սխեման, մշակված մեթոդների հիման վրա:

Աշխատանքի հիմնական արդյունքները հետևյալն են՝

- Մշակված է մատնահետքի պատկերի լավարկման մեթոդ, որը կբարձրացնի հատուկ կետերի առանձնացման գործընթացի որակական չափումները:
- Ներկայացված է հատուկ կետերի առանձնացման սխեման և գնահատված է երկու որակական չափումներով զգայունություն և յուրահատկություն: Արդյունքների վերլուծությունը ցույց տվեց, որ զգայունության և յուրահատկության բարձր արժեքները խոսում են սխեմայի արդյունավետության մասին: Դրանք ցույց են տալիս ներկայացված սխեմայի, մատնահետքի պատկերում իրական հատուկ կետերի հայտնաբերման և կեղծերի հեռացման ունակությունը:
- Առաջարկված է մատնահետքերի համար ոչ հստակ պահոցի բարձր գաղտնիությամբ սխեման, որն առկաների համեմատ նվազեցնում է հատարկման եղանակով հարձակումների արդյունավետությունը:
- Մշակվել են մատնահետքի պատկերի լավարկման և հատուկ կետերի առանձնացման համակարգի ծրագրային մոդուլներ, որոնք կարող են օգտագործվել մատնահետքերի ճանաչման տարատեսակ կիրառումներում:
- Մշակվել է FuzzyVault համակարգի արդյունավետ հետազոտություններ և վերլուծություն ապահովող հետազոտական ծրագրային համակարգ, մատնահետքից հատուկ կետերի հայտնաբերման ավտոմատացված համակարգի կիրառմամբ:
- Մշակվել է մատնահետքի հիման վրա ոչ հստակ պահոցի համակարգ, որն ապահովում է տվյալների բարձր անվտանգություն և ավելացնում է համակարգի կոտրման համար անհրաժեշտ գործողությունների քանակը գրեթե 30 անգամ:

Мага Саад Аль дин Мохамад Толба

РАСПРЕДЕЛЕННАЯ ЗАЩИТА ДАННЫХ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ

РЕЗЮМЕ

Поскольку наша повседневная жизнь становится более компьютеризированной, автоматизированные системы безопасности становятся более важными. Например, сегодня большинство банковских операций выполняются по Интернету. Из-за растущей важности информационных технологий, потребности защиты данных и ограничения доступа, необходимо надежное установление подлинности личности.

В сегодняшнем развитом мире цифровых технологии есть увеличенная потребность в безопасности, приводящая к развитию многих основных систем опознавания личности. Основная задача системы аутентификации состоит в том, чтобы подтвердить, что пользователи являются теми, кем представляются. Существуют три основные методологии, для выполнения проверки. Система безопасности может запросить: предоставить некоторую информацию, известную только пользователю, либо предоставить кое-что, к чему только у пользователя есть доступ, или же идентифицировать особую черту, которая уникальна для пользователя. Идентификация особой черты, которая уникальна для пользователя, известна как биометрическая безопасность. Биометрическая система - система распознавания образов, которая устанавливает подлинность определенной физиологической или поведенческой характеристики, представленной пользователем. Отпечатки пальца - наиболее широко используемый параметр в биометрии. Причина популярности распознавания на основе отпечатке пальца - неизменность отпечатков пальца в течении человеческой жизни и их уникальность.

Проблема защиты данных - одна из различных типов проблем безопасности. Защита данных возникает от потребности хранить важную информацию от потери, уничтожения или попадания в чужие руки. Современный подход к решению этой проблемы предлагает объединить криптографию и биометрию. Слияние между ними привело к развитию шифровальных конструкций, где секретные данные защищены, используя биометрические характеристики. Одна из шифровальных конструкций - схема нечеткого хранилища на основе отпечатка пальца. У этой конструкции есть некоторые недостатки безопасности. Местоположения точек в хранилище могут раскрыть некоторую информацию, относительно которой точки являются подлинными в зависимости генерации лонных точек. Другой недостаток состоит в том, что конструкция уязвима для атаки методом перебора.

Основная цель исследования

Основная цель и задача работы заключается в том, чтобы исследовать и разработать принципы повышения продуктивности и секретности схемы нечеткого хранилища использующегося для защиты секретных данных. Так как схема основана на отпечатке пальца, другая задача заключается в разработке высококачественной системы для извлечения минуций из отпечатка пальца.

Для достижения данной цели в работе необходимо решить следующие задачи:

1. Исследовать качество изображения отпечатка пальца и получить методы повышения продуктивности процесса улучшения отпечатка пальца.
2. Спроектировать и разработать модель для извлечения минуций из отпечатка пальца, что позволит найти расположение истинных минуций в улучшенном изображении отпечатка для повышения продуктивности конструкций нечеткого хранилища.

3. Исследовать и разработать методы для исправления недостатков и уязвимостей конструкций нечеткого хранилища.
4. Разработаны новые алгоритмы и соответствующие программные средства, которые реализуют схема нечеткого хранилища на основе разработанных методов.

Основные результаты работы:

- Разработан метод улучшения качества изображения отпечатка пальца, что повысило качественные измерения процесса выделения минуций.
- Представлена модель извлечения минуций и оценена с использованием двух качественных измерений, чувствительность и специфичность. Высокие значения чувствительности и специфичности указывают на эффективность модели. Они показывают способность представленной модели выявить истинные минуциии и удалять лживые минуции в изображении отпечатка пальца.
- Разработан метод конструкции нечеткого хранилища с высокой степенью секретности, который по сравнению с существующим понижает вероятность успешной атаки методом перебора.
- Разработаны программные модули предназначенные для улучшения изображения отпечатка пальца и системы извлечения минуций, которые могут использоваться в разных приложениях распознавания отпечатков пальцев.
- Разработана исследовательская программа, обеспечивающая эффективные исследования и анализ системы FuzzyVault используя систему автоматического извлечения минуций из отпечатка пальца.
- Разработана система нечеткого хранилища на основе отпечатка пальца, которая обеспечивает надежную защиту данных и увеличивает количество необходимых операций для взлома системы почти в 30 раз.