Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.8, 2015
www.iiste.org

Bio-cryptography using Zernike Moments and Key Generation by Cubic Splines

Ahmed Abdulrudah Abbass[1*] Wesam Bhaya [2]
1. Education College, University of Kufa, Najaf, Iraq
2. IT College, University of Babylon, Babylon, Iraq

Abstract
Cryptography is the process of protecting sensitive information and making it unreadable to unwanted parties. Since all algorithms that perform this task depend on the process of finding a suitable key, the key generation is considered the soul of powerful encryption. The traditionally generated keys are long and random, hence are difficult to memorize, and we need a database to store the keys. To alleviate this limitation, we use bio-cryptography that is combined of biometrics and cryptography. Using Bio-Cryptography generated keys provides the necessary security through powerful encryption and decryption of data. This paper uses cubic spline to generate a cryptographic key through extracting the features from fingerprint. The approach is based on extracting the features generated by using Zernike Moment on a biometric, and then sending these features to a Cubic-Spline Interpolator to generate the keys. A key encryption will be generated for every person through extracting the features from his / her biometric (fingerprint) and then applying these features on the cubic spline interpolator to obtain some points. These interpolated points will be used as keys to encrypt the information by using a suitable encryption algorithm. The benefit presented by this approach is to ensure a high level of security to protect the information through generating secure keys ready to be used for unsecured channel. In this paper, we used fingerprints from Biometric Recognition Group - ATVS to examine the performance of this approach.
Keywords: Biometrics, Key Generation, Zernike Moment, Cubic Spline, Cryptography, RSA, Fingerprint.

1. Introduction

Biometric security systems can identify individuals using bio-physical characteristics of humans such as voice, iris, ear, gait and fingerprint [Mingwu Zhang et al. 2011]. In the last two decades there has been an increasing interest in the use of biometrics in security applications (e.g., for authentication). After several significant works, cryptography and biometrics have been crystallized as biometric cryptosystem [U. Uludag et al 2004]. There are two ways of using biometric key. These are Biometric-based key generation for cryptography.

Biometric matching.

For former case, biometrics as well as saved templates are utilized in the creation of the secret key [R.Seshadri et al. 2010]. This approach has be considered by many researchers in recent years.

Hanaa M. A. Salman [Hanaa M 2012] proposed a solution for various types of security problems by introducing a fuzzy bio-cryptography key generation. It is composed of: 1. Sensing, 2. Feature extraction, 3. Key generation. The key is generated dynamically with the help of fingerprint based cubic spline, which is fast and secure. This key is useable for any type of cryptography.

Mingwu Zhang [Mingwu Zhang et al. 2011] proposed a multi-biometric encryption and authentication scheme. The scheme proved to be secure in the random oracle model. In this scheme, secret key is generated based on multi-biometric data extraction (by biometric string reader) followed by fuzzy extraction. The proposed scheme can be used in biometric based authentication.

Hu, Cai Li [Peng Zhang et al. 2011] studied the effects on the generated keys caused by rotation of an original fingerprint image. The study showed that the details of original fingerprint image can be obscured by image rotation. They also showed that the quantization and interpolation process can have a damaging effect on the fingerprint but without any significant effect on the visual image.

Jagadeesan et al [J. Jagadeesan et al. 2010] proposed multi-modal biometrics (based on both iris and fingerprint) for key generation. The security is later enhanced during the ciphering process with the difficulty of large number factorization. At first, the delicate features are extracted from the fingerprint and iris. Then, these features are used to get the multi-biometric. Finally, this multi-biometric template is used to generate a 256-bit key.

Throughout the above works when the researchers deal with fingerprint the rotation of fingerprint is neglected and therefore this will give a difference of the features from original fingerprint. This feature will give different keys compared to the one extracted from original fingerprint. Motivated be the above factors and to overcome these limitations, we propose a new method of cryptographic key generation from fingerprint using Zernike moments and cubic splines to generate the key used in the RSA algorithm. In this proposed method we used the Zernike moment which is rotation invariant to overcome this issue. Also, we didn't regarded the features as encrypted keys but rather using these features in cubic spline interpolation to generate the points and

from these points we will select the prime number (***p*** and ***q***) that will be used in RSA algorithm to obtain the public and private key.

The proposed method can be summarized as follows:

Firstly, we extract the features from the fingerprint by taking Zernike moments of its image, where at least eight values (features) are extracted using Zernike moment. There are good features of Zernike moment that will help in generating a strong encryption key. These features will be considered as points (with ***x*** and ***y*** coordinate), which we apply to a cubic spline process to draw a specific curve for the person under test. Every person will have a distinct curve. From this curve, we obtain thousands points for that person. These points never repeat (while using the algorithm for other persons) because this process depends on the person's biometric. Therefore, from these points we detect the specific keys that will be used in the RSA algorithm. These keys must be prime when both x and y are is primes ***(x',y')***. As such, this approach can generate powerful keys that maintain high level of security to protect information through unsecure channels.

For performance testing we applied this approach on the Biometric Recognition Group - ATVS database of fingerprint [ATVS 2006].

2- RSA Algorithm Description

The RSA algorithm is a strong ciphering algorithm that is based on public key and uses block ciphering. RSA algorithm utilizes a pair of keys: a public key which known for all, is used to encrypt the plain text, and a private key, which is used to decrypt the cipher text and this key must be kept secure [Ronald L et al. 1978].

In RSA, the public key is the product of two prime integers: ***n= p*q***, where ***p*** and ***q*** are large, distinct primes. Note that ***n*** is composite, not prime. To encrypt a message, two things are needed: the composite integer ***n*** and the public key ***e***. The public key ***e*** should be co prime with ***Φ(n)***, the Euler totient function. Now to decrypt the message, we need two things: ***n*** (same as that used for encryption) and a private key ***d***. This private key is the inverse of the public key e modulo ***Φ(n)***[Prashant Sharma et al. 2012].

3- Zernike Moments

For the few last decades, moments have been actively used for image processing and computer vision. If rotational invariance is required, moments defined over polar coordinates are used. Examples are radial moments and Zernike moments [Teh, C. 1988]. Teague was the first to introduce Zernike moments, based on orthogonal Zernike polynomials, to handle information redundancy in the popular geometric moments [Teague 1980]. Zernike moments proved to be effective in image representation. Zernike moments are rotation-invariant. Arbitrary orders of these moments can be found. Higher order moments may reveal fine details of the image; however, they are more susceptible to noise [Heloise Hse 2004]. Generally, Zernike moments have been proven to be more robust against Gaussian noise [Seyed Mehdi Lajevardi et al. 2009]. In combating redundancy, Zernike moments can to achieve a near-zero redundancy, mostly due to the fact that their moment functions are defined using polar coordinates [Chee-Way Chong et al. 2003].

Zernike moments are defined based on Zernike complex polynomials which form a complete orthogonal set over the interior of the unit circle, i.e., $x^2 + y^2 = 1$. If we denote these polynomials by $\{V_{nm}(x, y)\}$, then their general form is given by:

$$V_{nm}(x, y) = V_{nm}(p, \theta) = R_{nm}(p)e^{jm\Theta} \qquad (1)$$

where

$$j = \sqrt{-1}$$

n non-negative integer

m integer (positive and negative) subject to the condition n-|m| even, $|m| \le n$

p length of vector from origin to (x,y), hence $p = \sqrt{x^2 + y^2}$.

θ angle between vector p and x axis in counterclockwise direction, hence

$$\theta = \tan^{-1}\left(\frac{y}{x}\right)$$

$R_{nm}(p)$ Radial polynomial defined as:

$$R_{nm}(p) = \sum_{s=0}^{\frac{n-|m|}{2}} (-1)^s \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!} p^{n-2s} \qquad \dots (2)$$

The Zernike moment for an image $f(x, y)$ of order n with repetition m is given by:

$$A_{nm} = \frac{n+1}{\pi} \sum_{x,y} f(x, y)V_{nm}(x, y); \quad x^2 + y^2 \le 1 \quad \dots . (3)$$

Zernike moments for a rotated image differ from those of the original un-rotated image in phase shifts only, not

in magnitudes. Therefore $|A_{nm}|$ can be used as a rotation invariant feature of the image function [Khotanzad, A 1990 ;, Seyed Mehdi Lajevardi et al. 2009].

4- Cubic Splines

For real-life data, it is difficult to find a function that can approximate the relation between these data. If such a function is found using interpolation methods, it will be very complicated and difficult to use. Cubic splines were proposed to interpolate real-life data efficiently [Rorres Chris 2005 ; Van Loan 1997]. However, the linear spline (straight line interpolation) is not continuously differentiable due to discontinuity, and the interpolating graph will not be smooth. The quadratic spline has a curvature that changes abruptly at each data point(x_i, y_i), hence it fails to follow corners efficiently. The most successful splines are the cubic splines (composed of polynomials of third degree). Nevertheless, the third derivative of a cubic spline function is discontinuous. Hence, when there are more than four points to be interpolated, the cubic spline through successive sets of four points will also be discontinuous in slope at the endpoints (knots) where different cubic curves meet. Still we have continuous first and second-order derivatives at the knots [David Kahaner et al. 1989].

The cubic spline S has several merits to be widely used in image processing and general data interpolation purposes:

1- When S, S' and S" are continuous, then splines looks friendly to the eye due to smoothness.
2- The conditions involved are not difficult to reach in many applications.
3- Generally, odd polynomials have better properties.
4- Cubic Splines are widely studied and available [David Kincaid 2004].

The basic idea of cubic spline interpolation is to fit to a set of data a piecewise polynomial function of the form

$$S(x) = \begin{Bmatrix} S_1(x) & \text{if} & x_1 \le x \le x_2 \\ S_2(x) & \text{if} & x_2 \le x \le x_3 \\ \vdots & \vdots & \vdots \\ S_{n-1}(x) & \text{if} & x_{n-1} \le x \le x_n \end{Bmatrix} \quad \dots\dots\dots\dots\dots (4)$$

where S_i is a third-degree polynomial defined as follows:

$$S_i(x) = a_i(x - x_i)^3 + b_i(x - x_i)^2 + c_i(x - x_i) + d_i \quad \dots\dots\dots\dots\dots\dots\dots\dots (5)$$

The system in (2) represents $(n-1)$ equations. The first and second derivatives of these equations are given by:

$$S'_i(x) = 3a_i(x - x_i)^2 + 2b_i(x - x_i) + c_i \quad \dots\dots\dots\dots\dots\dots\dots\dots (6)$$

$$S''_i(x) = 6a_i(x - x_i) + 2b_i \quad \dots\dots\dots\dots\dots\dots\dots\dots (7)$$

5-Experimental Setup

This section describes the experiment performed to evaluate the proposed approach.

Figure (1) shows a block diagram of the proposed encryption system. The system involves a new method to generate a key from a fingerprint by extracting the features represented by Zernike moments. After preprocessing (enhancement), we compute the eight magnitudes of Zernike moments. These features are designated as data points $\{(x_i, y_i)\}$ that will be used by the cubic spline interpolator to generate a key for the encryption algorithm.

5.1. Fingerprint Image Enhancement (Preprocessing):

The first step in the processing of the fingerprint image is to convert it to a gray image with levels (0-255). Most of the image information is represented in the gray version of the image.

Fingerprint Image enhancement is used to make the image clearer and easier when processing using further operations. Note that the fingerprint images acquired from scanner or any other media may not be good enough quality, also, it may include some noise from various sources. Enhancement methods are necessary to keep a high level of accuracy image features. As these features will be used for key generation, we need a highly accurate approach for better security. In this paper we attempted the following image enhancement stages.

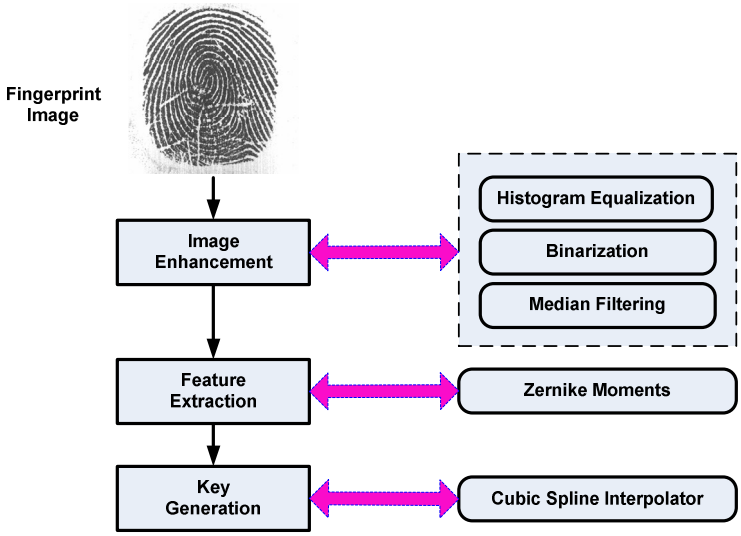

Figure 1. Diagram of the Proposed Encryption System.

5-1-1 Histogram Equalization:

Histogram equalization is the process of re-arranging the distribution of illumination levels in an image into more uniformly-distributed values so as to increase the perceptional information. Figure (2a) shows the original histogram of a fingerprint image, while Figure (2b) shows the histogram after the equalization process.

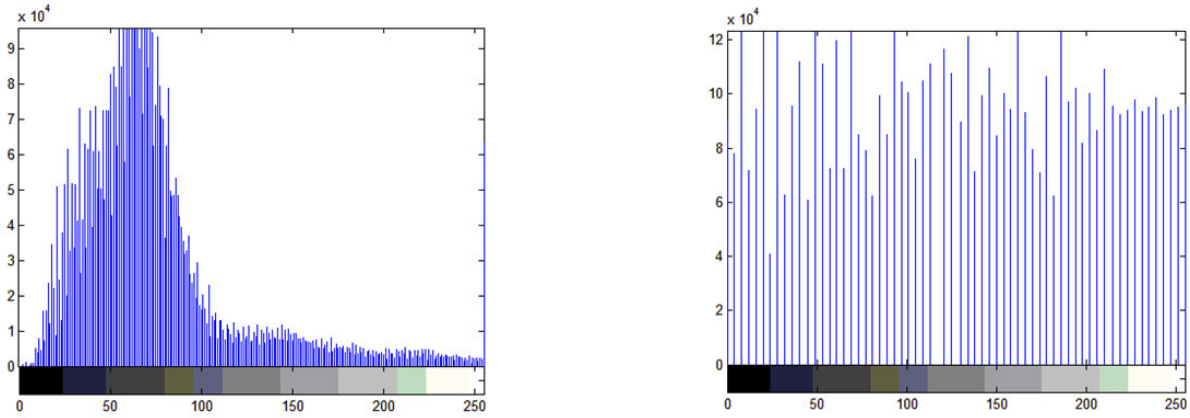

Figure 2. (a) The original histogram of a fingerprint image.
(b) The histogram after the histogram equalization.

(a) (b)

Figure 3. (a) The original fingerprint image. (b) After histogram equalization.

The original fingerprint image is shown in Figure (3a), the fingerprint after the histogram equalization is shown in Figure (3b).

5-1-2 Fingerprint Image Binarization:

Noting that the true information inside the fingerprint image is mostly binary in nature, hence we can use only a binary version of the fingerprint to reduce time complexity and make the proposed system more efficient for real-world applications. The process of binarization will transform the image from a 256-level image to a 2-level image, keeping almost the same original information.

Typically, a pixel that is part of an image object becomes binary “1”; while a background pixel

becomes "0". Hence, the final binary image will be composed of two colors only: white (for "1") or black (for "0").

The fingerprint image after histogram equalization is shown in Figure (4a), and the fingerprint after the binarization process is shown in Figure (4b).

5-1-3 Median Filtering:

Noise is a companion of image acquisition. After apply the above steps, we now must remove noise from the fingerprint by applying the median filter. The reason for using median filtering is to remove impulsive noise that may affect Zernike Moments, hence compromising the efficiency of ciphering.

Figure 4. (a) Histogram equalization fingerprint image.
(b) Fingerprint after the binarization.

Note that Zernike moments, although resistive to Gaussian noise, are affected significantly by impulsive (salt and pepper) noise. After median filtering, the image will be ready for key production. Figure (5) illustrates the filtered image that can be used to extract the important biometric features.

5-2 Extracting the Features and Applying Cubic Spline:

After enhancing the fingerprint, now we can extract Zernike features from the fingerprint by applying the Zernike moments. These features will represent the points to be used in the cubic spline interpolator. When applying the Zernike moment, we intend to extract eight features. Each pair of these features will represent a data point $\{(x_i, y_i)|i = 1:4\}$ on the curve to be approximated by the cubic spline.

Figure 5. Fingerprint after Median Filtering.

For example, if we apply Zernike moment on the first fingerprint in this test, labeled as F1, must be in the beginning detected the value of p and q which represent the order and repetition of **Z** moment where $p \leq q$ and $|p-q|$ is even. Therefore, in our test we detected the usability of the value of $p=1$ and the value of $q=4$ to obtain eight values of Zernike moments as illustrated in the table below.

Z11	Z20	Z22	Z31	Z33	Z40	Z42	Z44
8.04302	67.21181	23.19248	4.06911	2.35457	23.14750	3.93178	8.26853

After extracting eight values from Zernike moment we multiply these values by 100000 to extend their values (magnitudes) of Zernike moments, then round the result to remove the decimal point, and then reorder as follows before applying the cubic spline interpolation. Reordering will take the first four values of Zernike moment to represent the x coordinate and the other four values to represent the y coordinates. Each pair of these values represents one of four points that will be interpolated by the cubic spline as follows:

[(406911, 235457), (804302, 2314750), (2319248, 393178), (6721181, 826853)]

The result of applying cubic spline interpolator for F1 and other four fingerprints (F2, F3, F4, and F5) is illustrated in Figure (6).

Other values for p and q can also be chosen.

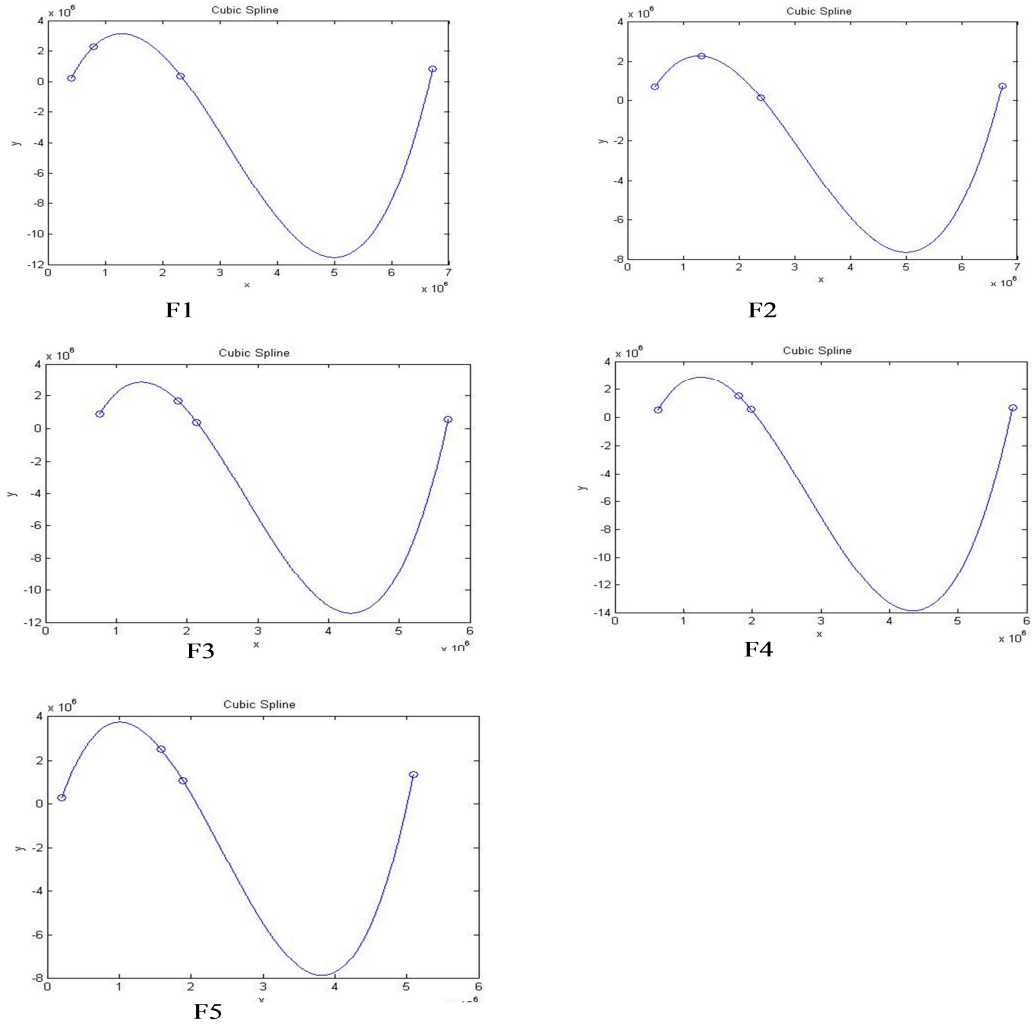

Figure 6. Five Results for Cubic Spline; each represents a Fingerprint.

6-Results

In this section we discuss the results of the proposed algorithm. The proposed algorithm is implemented using MATLAB. Table (1) illustrates the values for each fingerprint when the value of x and the value of y represents the value of Zernike moment, and the column of points of cubic spline are represent the samples of points which will detected the keys from it that will used to encrypted the data.

Table 1. The Value of Zernike Moment and samples Points of Cubic Spline for Five Fingerprints.

No. of Fingerprint	Value of x	Value of y	Points of Cubic Spline
F1	406911	235457	(419540,323359), (444797,494667), (514254,935261), (539511,1084551), (646853,1655671),(766824,2176547), (1303537,3143863),(4890043,11499461),…
	804302	2314750	
	2319248	393178	
	6721181	826853	
F2	495147	722575	(551281,945544),(557519,969141), (601179, 601179),(657313, 1315335), (669787,1354523),(1012831,2097769), (1118863,2205418),(1324689,2266049)…
	1329777	2265199	
	2400473	135521	
	6732305	750831	
F3	764034	883845	(783749,1018287),(793607,1083533), (966113, 2019096),(1054831,2355209) ,(1064689,2386763,(1104119,2501688), (1355486,2833802),(1754716,2134665)…
	1873418	1688344	
	2136574	395235	
	5692802	560475	
F4	627832	501012	(663991,780605),(679487,894564), (741473,1315825),(927431,2261523) (1030741,2592708),(1185707,2849655), (1247693,2876759),(2931647,6562279),…
	1803408	1490373	
	1980280	551401	
	5793337	683208	
F5	203547	276974	(286633,993639),(291521,1032885), (389269,1751842),(438143,2065337), (540779,2627947), (638527,2375931), (677627,3186217),(3575867,7633579), …
	1581259	2491617	
	1887514	1051413	
	5090967	1308608	

To encrypt the data by using RSA algorithm using encryption keys that we obtained from cubic spline, these keys must be prime numbers. From the four points that we found, we choose a pair (x',y'). If this pair is primes (tested using MATLAB isprime function), then it is the correct choice for RSA. If not, we modify the pair towards the nearest primes.

Table (2) illustrates some examples for the points of prime number from fingerprints that tested above.

Table 2. Examples of Points for prime pair (x',y') that represents p and q in the RSA Algorithm.

No. of Fingerprint	Points of prime number (x',y')
F1	(1303537,3143863),(4890043,11499461),(5635127,10114493),…
F2	(669787,1354523),(1012831,2097769),(1368349,2255233),…
F3	(1054831,2355209),(1064689,2386763),(1616711,2526317),…
F4	(932597,2281267),(1247693,2876759),(2931647,6562279),…
F5	(677627,3186217),(3575867,7633579),(4484927,5664101),…

After detect the prime point then we can use the x' as a p and y' as a q to get the public key and private key in the RSA algorithm in the step of generate key to encrypt the data. From the table above we can see that it is possible to choose a unique pair of encryption keys for each person by using his/her fingerprint. This approach will make it difficult for the attacker to predict the key as it depends on the biometric, giving a high level of security for the user information transfer through insecure channel.

Most of the research is this area focuses on obtaining the prime number using Random Number Generator (RNG) or Pseudorandom Number Generator (PRNG). These two ways may be have periodicity. Therefore, to riddance this periodicity we proposed a new method depending on biometric (fingerprint). This fingerprint is unique for each person, also we used the Zernike moment to extract eight features and then using these features as a control points to draw the curve by applying cubic spline interpolation and from points of curve we can select tow prime numbers (x' and y') as a p and q which will be used in RSA algorithm. Therefore, when we apply this method it gives a high level of security because the attacker cannot predict the encryption key. This key depends on biometric and cubic spline to obtain the prime numbers which is used in the RSA algorithm for generating the encryption key.

7-Conclusion

In this paper we propose new approach to generating the keys that is used in the RSA algorithm to protect the information, this approach summarized by extracting the eight features from fingerprint by using Zernike moment. The Zernike moments for a rotated fingerprint differ from those of the original un-rotated fingerprint in phase shifts only, not in magnitudes. Therefore $|A_{nm}|$th can be used as a rotation invariant feature of the fingerprint ;these eight values will be preprocessing such as multiplying each feature by factor to extend the value of feature and round it to remove the decimal point , after that reordering the four first values which representing the x coordinate and the others four values represent the y coordinate. Then this four points can applying cubic spline on it to draw the specific curve that represented the characteristics of this fingerprint, and

from this curve we obtained thousand points, from these points detected only the points that x is a prime and also the y is a prim (x',y') which will be using in the RSA algorithm to protect the information through encrypted it. These approach will gives a high level of security because the generated of keys are depending on biometric (fingerprint), extract the features by Zernike moment, and using cubic spline to obtain the encryption keys , therefore these keys will be unique for the specific person that can be used it to protect his / her information. Since, when the attacker attempt to break the ciphertext which generated by using this approach to generate key and RSA algorithm, he need the key, but the key cannot predict it, because it generated by our method.

References

Chee-Way Chong, P. Raveendran, R. Mukundan, (2003), "Translation invariants of Zernike moments PERGAMON", Pattern Recognition, 36 ,1765 – 1773.

David Kahaner, Cleve B. Moler, Stephen Nash, George Elmer Forsythe,(1989), "Numerical Methods and Software", Prentice–Hall, Englewood Cliffs, NJ,.

David Kincaid, Ward Cheney,(2004), "Numerical Mathematics and Computing", Fifth edition, Brooks/ Cole Publishing Company, Belmont, CA.

Hanaa M. A. Salman, (2012), "Fuzzy Bio-Cryptography Key Generation", The 13th International Arab Conference on Information Technology ACIT, pp.538-543, Dec.10-13.

Heloise Hse and A. Richard Newton,(2004) "Sketched symbol recognition using Zernike moment" , Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004, Vol.1, pp. 367 - 370.http://atvs.ii.uam.es/fvc2006.html

J. Jagadeesan, T. Thillaikkarasi, K. Duraiswamy, (2010), "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications, 2(6), pp. 16–26.

Khotanzad, A., and Hong, Y.H.,(1990)," Invariant Image Recognition by Zernike Moments", IEEE Trans. on PAMI, Vol. (12), No. (5), pp. 289-497.

Mingwu Zhang, Bo Yang, Wenzheng Zhang, Tsuyoshi Takagi,(2011), "Multibiometric Based Secure Encryption and Authentication Scheme with Fuzzy Extractor", International Journal of Network Security, Vol.12, No.1, PP.50–57.

Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula, (2011), "A pitfall in fingerprint bio-cryptographic key generation", Computers & Security, Volume 30, Issue 5, July 2011, pp. 311–319.

Prashant Sharma, Amit Kumar Gupta, Ashish Vijay, (2012), "Modified Integer Factorization Algorithm using V-Factor Method", Second IEEE International Conference on Advanced Computing & Communication Technologies, IEEE, pp.423-425.

R.Seshadri, T. Raghu Trivedi, (2010) "Generation of key for Session key Distribution Using Bio-Metrics", *IJCSE*, pp. 1992-1995, Vol. 02, No. 06.

Ronald L. Rivest, Adi Shamir, Len Adelman,(1978), "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, pp. 120-126, Volume 21, Issue 2.

Rorres Chris, Howard Anton,(2005), "Elementary Linear Algebra", Ninth Edition, John Wiley and Sons, New York.

Seyed Mehdi Lajevardi, Zahir M. Hussain,(2009), "Zernike Moments for Facial Expression Recognition ",International Conference on Communication, Computer and Power (ICCCP'09), Muscat, Oman, 15-18.

Teague, M.R., (1980)," Image Analysis via the General Theory of Moments", Journal of the Optical Society of America, 70 (8). 920-930.

Teh, C. and Chin, R.T.(1988), "On Image Analysis by the Methods of Moments", IEEE Trans. on PAMI, 10 (4), 496-513,.

U. Uludag, S. Pankanti, S. Prabhakar, and A. K.Jain,(2004), "Biometric cryptosystems: Issues and challenges", Proceedings of the IEEE, vol. 92, pp. 948-960.

Van Loan, Charles F,(1997), "Introduction to Scientific Computing", New Jersey: Prentice Hall.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar