International Journal of Electrical Sciences & Engineering (IJESE)
Online ISSN: 2455 6068; Volume 1, Issue 1; January 2016 pp. 13-18

Performance Measurement of Cryptographic Key using Biometric Images

Mohammed Tajuddin[1], C. Nandini[2]

[1]Associate Professor, Department of Computer Science and Engineering,
Dayananda Sagar College of Engineering, Bangalore
tajdsce@gmail.com
[2]Professor, Department of Computer Science & Engineering,
Dayananda Sagar Academy of Technology & Management, Bangalore
laasyanandini@gmail.com

Abstract: **The biometric field is one of the promising frontiers of scientific advancement in network security applications. Hence, the cryptographic key is generated using the retina biometric features. The Biometric features will improve the security of cryptographic system. In this paper, thinned vascular tree of retina biometric is used to generate the cryptographic key. This work emphasizes upon unification of features which enables to generate more secured cryptographic key. This work introduces a unique method to generate a secured cryptographic key for any network security applications. This technique of operations in network security creates more complexity for hackers to crack or guess the key. Thus, security is further enhanced using the above technique.**

Keywords: **Cryptography, Biometrics, Endpoints, Bifurcation, island, Morphological operation and vascular tree, Encryption & decryption**

1. INTRODUCTION

With the rapid growth of internet and the advancements of network communication technologies, the communication channel must be secure and protect the message send across the communication channel at the same time user expecting secure data transmission.

Many cryptographic algorithms are used which are simple and efficient to implement on high performance to convert the message into unintelligible message. Some cryptographic algorithms operation which takes few milliseconds in securing the messages, perform authentication and the integrity check on machine. Hence, it is critical to user to select the specific algorithm to provide maximum security. The primary objective of cryptography is to ensure provisioning of confidentiality, integrity and availability. The goal of confidentiality is data exchange between two users must be on trusted network, the information while exchange remains unchanged and secret. Integrity the information is always exchange between two users, but changes should be made by authorized users only [5]. Integrity prevents the modification and to detect any modification made to the message. The confidentiality and integrity should not hinder the availability of data. The data must be available to the authorized users only. Types of cryptography algorithms secret key cryptography, public key cryptography and hash function [19]. In secret key cryptography only one key is used for encryption and decryption while in Public key cryptography one key encryption and another key for decryption of message.

It is worth to recall that security has become an increasingly important factor with the growth of digital world. The Symmetric in which the same key value is used in both the encryption and decryption calculations are popularly used. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt the message in blocks of 128 bits.

- AES is used as it is simple to implement by using cheap processor and uses minimum amount of memory. It has better resistance against existing attacks and increases the security with less power and high throughput. AES uses four types of transformations namely substitution, permutation, mixing and key adding [7].
- AES such as DES uses substitution. However, the mechanism is different where the substitution is done for each byte.
- Another process found in a round is shifting. Shifting transformation in the AES is done at the byte level: the order of the bits in the byte is not changed [6].
- In encryption, the transformation is known as Shift Rows and the shifting is to the left.
- The mixing transformation changes the contents of each byte by taking four bytes at a time and combining them to recreate four new bytes.

- The functionality in the Add Round Key is matrix addition. Since addition and subtraction in this field are the same, the Add Round Key transformation is the inverse of itself.

Block cipher there are various modes of block cipher have been tested, the serve in this paper is AES [5].

Hash function several widely used hash function are evaluated such as MD2 [15], MD4 [16], MD6 [17] and SHA-1[18].

Cryptographic techniques are widely used for ensuring the secrecy and authentication of database information. The secure protection of information depends upon the cryptography key, which is only known to the authorized users. Maintaining the secret key is one of the challenging issues over the internet [7]. The security of information in encryption system is depends on the technique used to generate the secrecy key for encryption and decryption instead of the encryption algorithm. The encryption system is thus unable to protect the cipher text once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space [4]. Larger the size of the key space more time does the attacker needs to do the exhaustive search of the key space. Thus, the level of security is higher. In encryption, the key is piece of information which specifies the particular transformation of plaintext to cipher text, or vice versa during decryption.

Biometrics is an emerging field of technology using unique and measurable physical and behavioral characteristics that can be processed biometric features for identification of a person. The biometric attributes include facial appearance, fingerprint, gait, geometry handwriting, iris, retina, veins and voice. Retina biometric identification is an automatic method that provides true identification of the person by acquiring an internal body image which is difficult to counterfeit [1]. Retina identification has gained its importance in application in high security environments. Retina biometric is unique biometric pattern that can be used as part of a verification system.

The rest of the paper is organized as follows: Section II provides the brief description of a generation of key from retina biometrics. Section III provides the background principles related to the working of the proposed model. All experimental results and related discussion is provided in Section IV. This paper is concluded by summing up the work in Section V.

2. II GENERATION OF KEY USING RETINA BIOMETRIC:

Biometric features such as the number of end points, the number of bifurcation points and the number of islands [25]. The above features are unique to all the retina biometric images, which is the unique method to generate the cryptographic key for encryption and decryption of message using cryptography algorithms. Accept the retina biometric from the database, convert the retina biometric to gray image, the values of gray image in the range 0 to 255 and then gray image to binary image in the form of 0's or 1's. From the binary image extract the blood vessels by setting the threshold value, the resultant tree is known as vascular tree as shown in Figure (2).

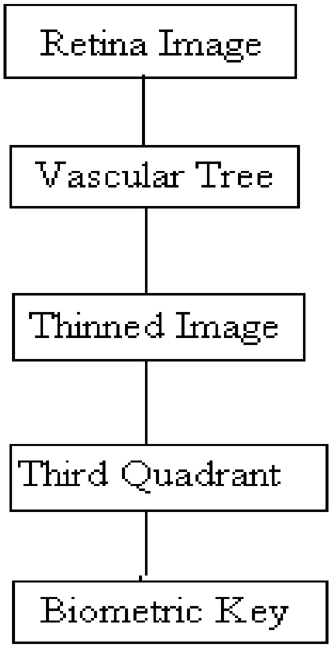

Fig. 1. Design Diagram

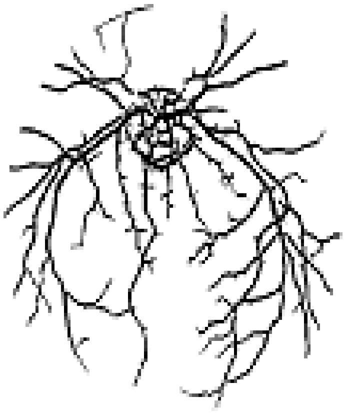

Fig. 3. Vascular Tree from the retina image

Next activity is to thin the generated vascular tree by using morphological operation such as dilation, erosion and open etc. the broad blood vessels are converted to thin line connected components, since we can find the end points from the thinned image as shown in Figure 3.

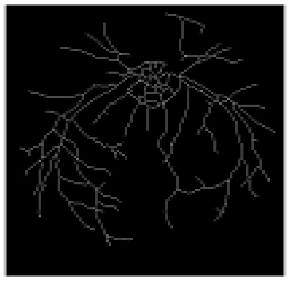

Fig. 3. Thinned vascular tree

Figure 3 indicates the number of end points, number of bifurcation points and the number of islands. Further divide this image into for quadrants, and then select the 3rd quadrant which has unique features as shown Figure 5, with reference to Figure 5.

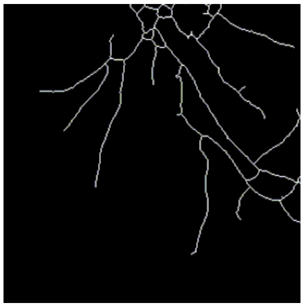

Fig. 5: 3rd Quadrant of a thinned image

Figure 5 has the unique features compare to the remaining quadrants of the thinned image as shown in Figure 3. Find the number of end points, bifurcation points and the islands. Key calculation of number of end points is by using 8 pixel neighborhood structuring element which is further depicted in Figure 4. Move the structuring element from the origin pixel by pixel to find the connect components of a line, if the structuring element unable to find the neighbor element with 1 indicates a end point and the counter will increment by 1 and the pixel coordinate x and y axis with angle will be considered as shown in Table 2.

The same image is further investigated to identify the number of bifurcation points. As per the conventional assumption to detect a line is to check for two adjacent pixel values to be 1. Applying the same principles here, the number of bifurcation points is obtained for the image. Table 3 indicates the bifurcation points, x and y values for those points using MATLAB code. Table 3 thus indicates that for the sampled retina image there exist 16 bifurcation points with the process of detecting end points and bifurcation points from the retina image [19].

1	1	1
1	1	1
1	1	1

Fig. 4. Structuring element 8 pixels

Finally, find the number of islands in Figure 5 by using principal components analysis to find the island of an image and also find the sum of area of islands which is unique for each image as shown in Figure 5. The extracted features are unique, since these features generate a unique biometric key and it used to encryption and decryption using AES algorithm.

Key Generation method by using the three retina features such as number of end points with angle, Number of bifurcation points with three degree and the number of island with the sum of the island area.

The following steps are used to generate the unique biometric key.

1. Read in the input retina image.

2. Feature extraction such as retina blood vessels

3. Thinning using morphological operations

4. Divide the thinned image into 4 quadrants

5. Select the 3rd quadrant which has unique features compare to other quadrants.

6. Find the number of end points

   $k_1 = \sum_{k=0}^{n} [x^k * y^k]$

7. Bifurcation points

   $k_2 = \sum_{i=0}^{n} [x^i * y^i]$

8. K_3 is number of islands are 8 with these features we can generate the secured key for cryptographic applications.

9. Key = $k_1 * k_2 * k_3$

3. ENCRYPTION PHASE

In this paper, biometric features are used to generate biometric key for the cryptographic systems. In the encryption method the part of the retina biometric features are used to generate the cryptographic key, the generated biometric key is converted to 128 bit key. In symmetric cryptography, a same key is used for both the encryption and decryption process. According to this methodology, a key must be same to both encrypting and decrypting method [11]. For encryption and its reverse process, in this work we use the Advanced Encryption Standard (AES) algorithm [19]. The overview of the proposed retina encryption phase is shown in Figure 6.

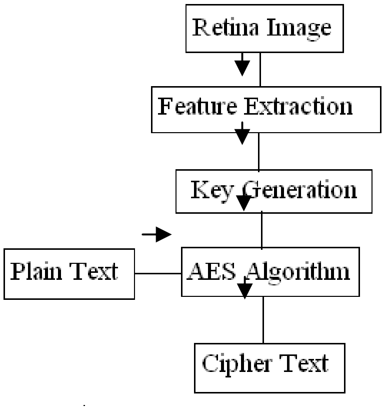

Fig. 6. Encryption phase using AES

The cipher text is the result of encryption performed on the plain text using an AES algorithm is called cipher. The cipher text is also known as encryption or encoded information because it contains a form of the original plain text which is unreadable by human or computer without the proper cipher to decryption using the same AES algorithm.

The generated cipher text again transforms back to original message by using decryption with AES algorithm as shown in Figure 7.

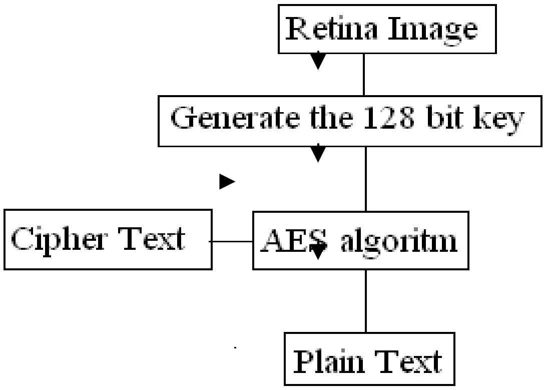

Fig. 7. Decryption phase

Results are obtained from different datasets such as DRIVE and stare. These are the following results such as number endpoints as shown in Table 2 from the origin.

TABLE 2: The number of end points

No	X	y
	284	41
	272	60
	194	63
	375	76
	235	111
	327	114
	120	119
	378	134
	327	142
	345	146
	145	159
	382	212
	363	224
	321	247
	323	248

TABLE 3: The Bifurcation points

No	X	y
	226	33
	254	36
	231	39
	290	40
	218	41
	299	43
	224	67
	192	85
	186	92
	263	94
	320	119
	262	141
	281	163
	342	200
	328	204

Table 3 illustrates the number of bifurcation points in Figure 5 and Table 2 show the number of end points in Figure 5, the complete code written in MATLAB. Finally the last feature numbers of islands in the 3rd quadrant are 8.

Performance measurement was tested to find the amount of time required to perform the encryption and decryption with different keys and different size of message with the existing method and our method. For each algorithm a number of tests are conducted where time taken is recorded as a sample time for each input message [20], Our approach execution time is less.

Rijindaels Functions: Table 4. Performance of AES

Key size	Message: 2KB		Message: 50KB		Message: 4 MB	
	Throughput (Bps)		Throughput (Bps)		Throughput (Bps)	
	Palm V	Retina	Palm V	Retina	Palm V	Retina
128	10673	10500	10711	10612	10522	10496
192	8989	8910	8947	8932	8769	8712
256	7764	7775	7673	7661	7516	7498

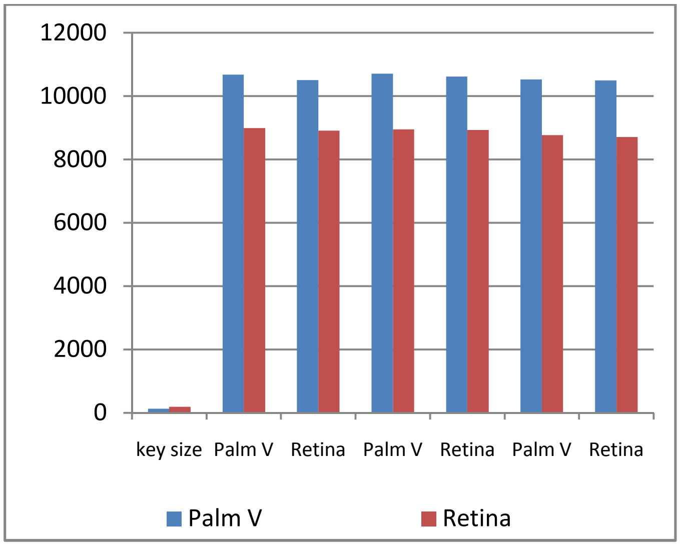

Figure 8: Comparison throughput of AES between palmv & Retina

DES Functions:

In this we also check the performance measurement results of DES with our approach, the performance of encryption and decryption with our approach results are better than existing methods [20]. We tested few samples with DES and the key is generated from the DRIVE dataset, Stare Data set for DES.

Hash Functions:

We also experimented with Hash function results of MD2, MD5 and our approach. All these algorithms are implemented in MATLAB library. The tested results are as shown in Table 5. By using hash function we found a bit improvement on the hashing speed for few hash functions [20], improvement in the range of 3 % to 5% with existing results. As we increase the size of the encryption and decryption time also increases tested with few key sizes. The results are as shown in Table 5.

TABLE 5: Performance of Hash

Hash	**Message: 2KB**		**Message: 50KB**		**Message: 4 MB**	
	Throughput (Bps)		Throughput (Bps)		Throughput (Bps)	
	Palm V	Retina	Palm V	Retina	Palm V	Retina
MD2	1738	1712	1747	1698	1739	1740
MD5	38102	37962	37647	37556	37608	37553
SHA-1	17429	17428	17770	-	17664	-

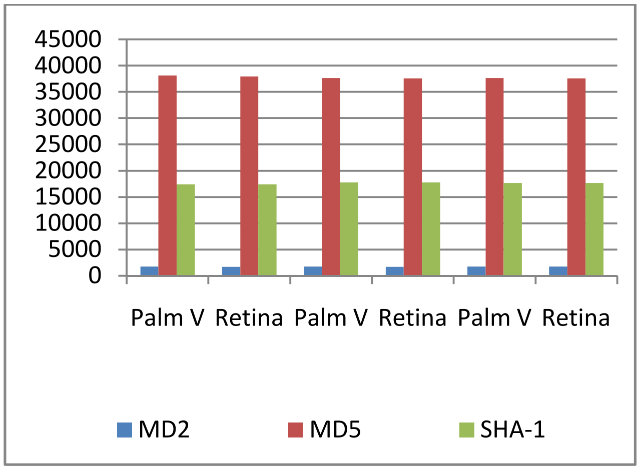

Fig.9. Comparison of throughput of Hash function between palm & Retina

4. CONCLUSION

The technique used to generate the cryptographic key is unique by using the retina biometric features. To generate the cryptographic key, more permanent features of the retina biometric are used such as the sub graph of vascular tree which has more permanent features compare to other quadrants in which the number of end points, bifurcation points and islands are used to create a cryptographic key for encryption and decryption of message. This paper has put forth the performance measurement comparison which is made between various existing cryptographic approaches and with variation in key and the size of messages. The comparative results has brought out the improvement of existing technique where instead of considering the complete image, it is now possible to generate the key by considering the part of the thinned image which has unique features.

REFERENCES

[1] Hill, R. B. 1978. Apparatus and method for identifying individuals through their retinal vasculature patterns, US Patent No. 4109237

[2] Chih-Peng Fanand and Jun-Kui Hwang, "FPGA Implementations Of High Throughput Sequential And Fully Pipelined AES Algorithm" International journal of Electrical Engineering, vol. 15, no. 6, pp. 447-455, 2008.

[3] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, "Efficient and High Performance Parallel Hardware Architecture for the AES-GCM" IEEE Transactions on Computers, vol. 61, no. 8, August 2012.

[4] A. A. Zaidan, A. W. Naji, Shihab A. Hameed, Fazidah Othman and B. B. Zaidan, " Approved Undetectable-Antivirus Steganography forMultimedia Information in PE-File ", International Conference on IACSIT Spring Conference (IACSIT-SC09), Advanced Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session 9, P. P 425-429.

[5] Behrouz A. Forouzan, "Cryptography and Network Security", *Tata McGraw-Hill*, 2007.

[6] Ramya M., Muthu Kumar A., KannanS. "Multibiometric Based Authentication Using Feature Level Fusion", *IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012)*, pp. 203-207, Mar 30, 31, 2012.

[7] R. Jubiaya, M Keirthi, "IRIS Authentication Based on AES Algorithm", IJIRSET, Volume 3, special issue 3, March 2014.

[8] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm", IEEE Transactions on Very Large Scale Integration Systems, vol. 12, issue 9, pp. 95 967, Sep. 2004.

[9] J. Vijaya, M. Rajaram, "High Speed Pipelined AES with Mixcolum Transform "European Journal of Scientific Research" 2011. Vol. 61 No. 2, pp. 255-264.

[10] C. Nandini & B. Shylaja " Effective Cryptographic Key Generation from Fingerprint using Symmetric Hash Functions", International Journal of Research and Reviews in Computer Science, Vol 2, No 4, ISSN 2079 - 2557, Aug 2011. Mohammed Tajuddin, C. Nandini, " Cryptographic Key Generation using Retina Biometric Parameter", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013, ISSN: 2277-3754.

[11] **Mohammed Tajuddin, C. Nandini, "More Secured Cryptographic Key Generation through Retinal Biometric using EBI Algorithm**

[12] Kai- Shun Lin and Chia-Ling Tsai, " Retinal Vascular Tree Reconstruction with Anatomical Realism", IEEE transaction on Biomedical Engineering, Vol 59, No 12, December 2012.

[13] Stallings, W. : Cryptography and Network Security, Prentice Hall, (2010).

[14] B. S Kaliski, Jr RFC 1319: The MD2 Message Digest Algorithm, IETF RFC 1319 Apr 1992.

[15] Ronald Rivest, RFC 1320: The MD4 Message Digest Algorithm, IETF RFC 1320 Apr 1992.

[16] Ronald Rivest, RFC 1321: The MD5 Message Digest Algorithm, IETF RFC 1321 Apr 1992.

[17] NIST FIPS PUB 180-1 Secure Hash Standard, Apr 1995.

[18] Mohammed Tajuddin, C. Nandini "Secured Crypto Biometric system using Retina", International Advanced Research Journal in Science, Engineering and Technology Vol. 2, Issue 1, January 2015.

[19] Duncan S, Wong, Hector Ho Fuentes and Angnes H "The performance measurement of cryptographic primitives on Palm devices", 2012 in CCS. NEU. EDU.