International Journal of Engineering Innovation & Research
Volume 3, Issue 5, ISSN: 2277 – 5668

More Secured Cryptographic Key Generation through Retinal Biometric using EBI Algorithm

Mohammed Tajuddin
Associate Professor, Department of Computer Science and Engg.,
Dayananda Sagar College of Engineering, Bangalore
Email: tajdsce@gmail.com

C. Nandini
Professor, Department of Computer Science & Engineering,
Dayananda Sagar Academy of Tech. & Management, Bangalore
Email: laasyanandini@gmail.com

Abstract **– Crypto Biometrics system is recently an emerging effective process to generate the keys and gaining high security authentication to validate the person verification by using biometric features. Biometric features will improve the security of cryptographic system. In such case, the stable cryptographic key should be generated from the biometrics. In this paper we are using retina biometric to generate the key, the key is directly generated from the human retina biometric information such as retinal blood vessels which is not stored in the database. This article presents three retina biometric features such as number of end points, bifurcation points and islands. This work emphasizes upon unification of these three features which enables one to generate the secured cryptographic key. This work introduces a novel algorithm named as EBI unification algorithm, which aims at the unification of the three features in order generate a more secured cryptographic key. This mode of operations in network security creates more complexity for hackers to crack. Also, it becomes highly difficult even to guess the cryptographic key or biometric key. This approach further reduces the cost associated with lost key and provides more security.**

Keywords **– Cryptography, Biometrics, Endpoints, Bifurcation, Island, Morphological Operation, Encryption and Decryption.**

I. INTRODUCTION

Since the times of civilization, communication has become one of the rudimentary modes of information exchange among the people. However, as civilization improved, technology started to play a role in the lives of the people. One such contribution to the human society is the introduction of computers. The progress of computer and technology has happened so enormously that it has led towards human computer interactions to go hand in hand for all the day to day activities of the society. Due to this fact, communication for information exchange through internet has become a vital organ.

Nevertheless, the advent in technology, there always prevail a threat to the information being hacked and thereby leading towards loss of important data. One of the challenges therefore is to provide security whenever information needs to get exchanged through the use of internet.

The field of cryptography involves studying of mathematical methods and techniques, which ensures a more protected communication whenever the communication encounters threat. Cryptography further emphasizes on various other aspects of providing information security such as confidentiality, data integrity, entity authentication and data origin authentication [17].

Implementation of cryptography algorithm should consider the important factors such as execution time, memory requirement, and computation power. In order to improve the performance of any cryptography algorithm, it is always better to incorporate parallel computation technique. Divide-and-conquer technique is deemed to be one of the popularly used methods for parallel computation to solve the algorithms in parallel which partitions and allocates the number of given subtask to available processing units [4].

Since communication is possible either through wired or wireless modes, it is required to provide security to both the modes of operations [23]. High speed security algorithms are used to achieve the above said objective. The aim of these algorithms is to encrypt the information such that security can be accomplished. Though, there exists symmetric or asymmetric mode of cryptography, the symmetric block cipher plays a major role in the bulk data encryption [1]. However, one of the best existing symmetric security algorithms to provide data security is advanced encryption standard. Security of the information depends upon the secrecy of the secret key or private key whether symmetric cipher approach or an asymmetric cipher approach [2]. Some of the most popularly applied cryptographic algorithms to secure the information include RSA, DES, 3DES and AES etc [17].

Despite of their strengths, every cryptographic algorithm suffers when the length of the keys is small, which is prone to easy guessing and hacking. Additionally, in conventional cryptography methods, the authentication of message is based on the key and is not based on the human components. Hence, there is a wide possibility of accepting the right key from the unauthorized user or attacker as key generation can be guessed or cracked. Other major inconvenience caused with key generation to achieve network security through cryptography is inherently complex nature of keys to remember and also the difficulty in storing them most securely in the database [4][5].

Since, the main motto of cryptography algorithms can be achieved through generation of secret key or private key, research has all the time dominated to proceed towards various methods of key generation. Some of the works where key generation has gained popularity is through password, random key generation, probability key generation, Bob Alice method, biometric approaches [12].

Biometric information is one of the popular methods for uniquely identifying an individual. Hence, this approach is adopted in key generation since it is now possible to generate keys uniquely through biometric sources which can be either physical or behavioral [9]. This technique ensures high security for applications using biometric features such as fingerprint, face, hand geometry, iris, signature, voice, retina and so on [6]. Instead of storing the key in the database, it is now therefore possible to generate the key dynamically using the biometrics.

Hence, crypto-biometric approaches, which combine biometrics with cryptographic methods, are gaining more and more attention towards identification and authentication of an individual. Person verification with high degree of assurance offered by biometrics can greatly improve the security of a cryptographic system. In such systems, a stable crypto-biometric key is generated from biometrics and a strong link between the user identity and the cryptographic keys is established [7].

Crypto-Biometrics approach has recently emerged as an effective means to resolve the issues faced by traditional cryptography system [8][9]. It is intended to find the key with the user biometric information in order to overcome the above-said issues through distortion, discrimination and security approaches.

Distortion is the ability to accommodate the variance of biometric [9]. The system which follows such crypto biometric approaches is expected to output the same key for the same user even if the biometric captured is at diverse conditions.

Discrimination is the ability of the system to distinguish all the users of the database and output different key for different users [9].

Security of the system ensures that neither the key nor the original biometric of the user can be traced or guessed and the user's biometric information is unique. Biometric based cryptography is therefore highly potential to provide security in advanced technologies.

Nevertheless, the existence of various methods of key generation, retina identification of crypto-biometric approach has proven to be one of the unique ways of key generation technique.

This research therefore focuses upon enhancing the effectiveness of key generation through retinal identification. The organ retina captures images that fall on its walls and the image gets identified through the signals sent from brain upon comprehending the image details sent by the retina to brain [24].

However, it is well proven that the structure of retina is stable and permanent which acts as unique for person to person [16]. This is because the network of blood vessels in the retina is so complex that identical twins do not even share a similar pattern. Hence, retina structure of an individual remains unique. Retinal based recognition for personal identification has desirable properties such as uniqueness, stability, non invasiveness, permanence, etc. Hence, Retinal identification technique is deemed to have the most precise and reliable biometric characteristics. However, the retinal blood vessel structure for biometric applications has not revealed its full potential. Further, retinal vessel vasculature has extraordinary structures and provides many interlacing characteristics, which also is unique for each person.

The organization of this article is as follows. Section 1 introduces the significance of secured communication achievable through crypto-biometric approaches. Section 2 provides details of works carried out by various researchers in this domain. Section 3 details the research work briefing the entire procedure carried out while Section 4 details the research carried out for generation of unique key through retina features. Section 5 gives the experimental results obtained upon the application of the research ideas on the data set collected for this purpose. Section 6 concludes the work carried out and presented as per this article is concerned.

II. Related Work

Several works has taken place in the areas of cryptography and biometric. Work has also carried out in the key generation for securing information through the integrated approach of above said techniques.

Network security has become a challenge for any organization whose internal private network is connected to the Internet, to perform the transaction over the internet. Network security safe guard is setup against unauthorized users access, alteration, or modification of information, and unauthorized denial of the service.

When a private network is connected to network that is at risk to potential intrusions and attacks. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology, which is important for network security [25].

Cryptographic key generation mechanism has proven to be one of the significant parameter to improve network security. Public-key algorithms are based on mathematical functions and are asymmetric in nature, involving the use of two keys, as opposed to conventional single key encryption. However, the major drawback of key generation approach to achieve security is that password can be lost, stolen or easily hacked [10][11].

Thus, the recent cryptographic application use of biometric based system information to generate unique key, have seen the exponential growth by using the biometric information such as fingerprint [12]. The fingerprint pattern which is stable throughout person's lifetime, thus the researchers are working in the domain of crypto biometrics since several years to achieve network security [6]. Work in the areas of finger print, palm and face recognition in addition to research in retinal biometrics is also observed. The finger print minutiae points, island and arc are used to generate the unique key. However, currently the research is popular in fingerprint biometric for the generation of key to achieve encryption and decryption of messages [6] [13].

There are several biometric systems in existence that deal with cryptography, but the figure print parameter based cryptographic key introduces a novel method to generate cryptographic key. This approach is implemented in MATLAB and can generate variable size cryptographic key, with minimum amount of time complexity, which is aptly suited for any real time cryptography [20].

The unique technique to generation of cryptographic key, the authors have used hashing technique in the finger trivia using completely different set of symmetric hash function for various users that is both secured and fast. The authors have extracted k-plets from every finger print image and calculate the hash values primarily based on the closest neighbor of a minutia purpose within the k-plet. A mix of those hash values are used to come up with a key [14].

With continues growth of the internet and the advancement of wireless communication system, the information send over the internet is not secured. An efficient approach to generate cryptographic keys is by using the patterns containing personal information. The cryptographic key generation may be identified by user features, and used by particular persons. In particular, key generation using palm images and coronary vessels will be presented [26].

However, retina biometric has proven to be one of the accurate modes of key generation feature, this work focuses upon retina biometric as an encryption key. The retina biometric features are unique and remain unchanged in lifetime.

- The strength of the retinal biometric recognition is better than all other biometric technologies. The blood vessels pattern of the retina rarely changes during the person's life (Unless disease or accident).
- The size of actual template is only 96 bytes, which is very small when compared to any standards in terms of verification and identification processing times, and is much shorter than they are for larger file.
- The rich unique structure of the blood vessels pattern of the retina allows up to 400 data points to be created.

Due to the above said unique biological characteristics of retina, the retinal recognition is primary used in combination with access control system at high security facilities. This includes military installations, nuclear facilities and laboratories [16].

The generation of cryptographic key using retina blood vessels pattern by counting the number of end points from the thinned image [15].

This research has thus progressed to enhance the previous work of the above said authors to integrate the bifurcation and island with end points towards unique key generation for secured cryptographic purpose.

III. Research Work

This research has focused towards generation of unique key through retina identification of crypto-biometric approach. The authentication process begins with the acquisition of required retina biometric template. Images for the retinal structure are obtained from various medical centers. These images are sample of various individuals. However, the information about the medical centers is collected as per the non disclosure agreement policy. The data set collected for this research comprises of large sample of 200 retinal images from 200 various age grouped individuals where the retina images represent both left and right eye.

Initial step involves extraction of the features from the retina biometric to generate a cryptographic key for cryptographic associated applications.

From the retina image obtained through the acquisition phase, the next step is to extract the features such as blood vessels pattern (vascular tree) which undergo the thinning process. Followed by the extraction process, subsequent step to be followed is identification of the endpoint of each pattern, to identify the bifurcation points and island. The thus obtained features are used to generate unique key. Figure 1 depicts the entire process of key generation using retina biometrics.

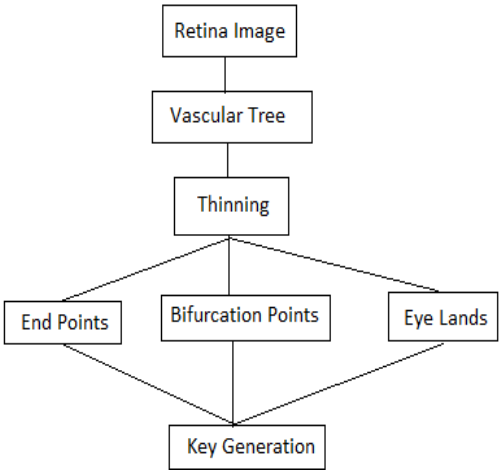

Fig.1. Design Diagram to generate the key

However, this paper limits to perform the investigation using grey scale images instead of colored image. MatLab programming converts the colored retina image to grey scale, which in turn converts grey to binary image using binarization technique.

Figure 2 depicts vascular tree which is converted to grey by using MATLAB code. Since, vascular tree contains large number of blood vessels, this work focuses upon the studying thick blood vessels. The main intention is to extract the thick blood vessels, which are major blood vessels in the retina and perform thinning operation using threshold value. The threshold value that is kept in this research is 1.39 as intensity value. This value is obtained as the optimized value after conducting various experiment with wide set of threshold values. The performance as obtained with various threshold values is further provided in subsequent sections of this paper. A blood vessel whose intensity is above 1.39 is therefore retained as it provides better resolution than those blood vessels whose intensity lies below the set threshold value [15].

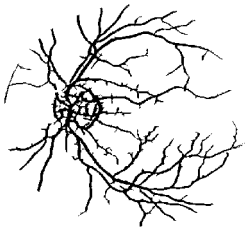

Fig.2. Vascular Tree

Having conducted the experiments to find the optimal threshold value to generate the structure of vascular tree, next step of this work is to segment the binary image by thinning process where pixels are eliminated from the boundary towards center without destroying the connection in an eight connected scheme, which is in compliance to the works carried out by the authors of [13].

Pruning process is further applied in this work to eliminate short, false spurs, due to small undulations in the vessels boundary. False spurs are deleted if they are smaller or equal to the largest vessels diameter expected in the particular image as shown Figure 2.

Followed by the retention of valid blood vessel pixels, the next step is to apply the Morphological operations in order to understand the structure or form of the image. This enables one to identify the boundary within the image. There are morphological functions such as Dilation and Erosion[27]. Dilation function is used to expand the image and erosion function shrinks the image in MATLAB code. Having obtained the boundary from the identified blood vessel, further work is to perform the thinning process. This process finds the center point in the vascular tree and compresses the boundary without disconnecting the other edges. Thinning is a morphological operation that is used to remove selected foreground pixels from the binary image [27].

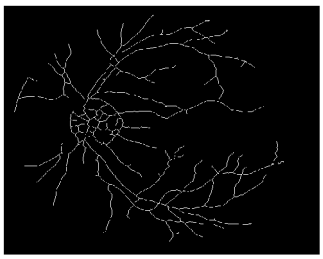

Fig.3. Thinned Image

Figure 3 Shows the thinned image which is obtained due to the morphological operations performed upon the vascular tree.

Following section describes the entire procedure incorporated towards more secured key generation through a novel approach of unification of End points, Bifurcation points and islands.

IV. The process of Unification of End Points, Bifurcation Points and Island for More Secured Key Generation

There are several works which has taken place towards the generation of secured key generation through either using only end points or works which has occurred using bifurcation points. Also there are related works which has indicated the amalgamation of endpoints and bifurcation points to generate cryptographic keys. This research has however proceeded towards unification of end points with bifurcation points in addition to introduction of islands present in retina structure which ensures a much better security towards generated key than the existing approaches.

4.1 End Point detection and bifurcation points from the thinned image

Upon the procedure of thinning the image, the next activity is identification of endpoint from the origin by using the morphological operation and the structuring element strategy. The objective of structuring element technique is to identify a pixel with value 1 as a termination point and no other pixels with that value in its neighborhood of 8 pixels should have 1. Such a pixel indicates an endpoint.

1	1	1
1	1	1
1	1	1

The structuring element will be thus moved from the origin of an image, pixel by pixel at a time in x and y axis. As structuring element match with the thinned image pixel, it finds an edge between two pixels, and continues this process for the entire image to find the number of endpoints in an image.

Figure 4 depicts the process of finding out end points and bifurcation points using MATLAB code for one of the sampled images which is collected for this research purpose. Figure 4 infers that whenever the structuring element does not match with the neighbor, the endpoint is set with red in color while green color indicates the bifurcation points.

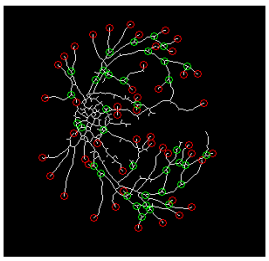

Fig.4. Endpoint and bifurcation points in thinned image.

Having collected the end points from the above mode, it is now required to find the coordinate values of each end point and degree theta is also considered indicating the angle in which the end point lies. Table 1 provides information about number of endpoints collected for a sampled retina image, x and y axis along with the theta angle of those end points. The Table indicates collection of totally 32 end points.

Table 1: Indicates the sample end points of thinned image.

Point	x	y	Angle
1	045	182	048
2	111	054	204
3	063	071	070
4	061	070	228
5	081	153	082
6	049	084	116
7	094	184	098
8	190	103	035
9	104	254	108
10	165	122	027
11	129	241	131
12	121	131	131
13	137	198	138
14	222	146	023
15	148	101	153
16	125	153	160
17	154	110	155
18	266	156	035
19	161	071	169
20	157	170	165
21	175	049	178
22	100	183	170
23	183	260	186
24	030	189	177
25	194	055	194
26	233	200	040
27	202	251	207
28	083	213	167
29	216	177	216
30	241	223	082
31	228	185	230
32	117	240	177

The Table 3 gives the angle when retina image is viewed from particular theta. However, this investigation is further progressed to find if the number of end points still remains the same when an retina image of an individual person is collected at various angles. Table 3. Provides the various angles at which the very same retinal image which is sampled and presented in this paper is rotated at various positions to validate the above assumption.

Table 2: Comparison of a single end point with different angles for the same sampled retina image

S.No.	Degree	X	Y	Angle3
1.	0	223	82	207
2.	10	209	104	223
3.	15	209	112	222
4.	20	210	119	183
5.	25	209	103	210
6.	30	186	131	211

Table 2 Therefore infers that whatever be the angle of rotation, the number of end points remains the same.

4.2. Bifurcation Point detection from the thinned image

The same sampled 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 2 indicates the bifurcation points, x and y values for those points using MATLAB code and also the theta angles which is viewed from three perspectives of bifurcation points. Table 2 thus indicates that for the sampled retina image there exists 17 bifurcation points.

Table 3: The number of bifurcation points with angles.

Bifurcation Point	X	Y	Angle1	Angle2	Angle3
1	078	079	078	107	085
2	141	090	146	104	192
3	106	089	115	149	112
4	201	115	078	118	124
5	121	083	122	056	138
6	090	142	228	149	192
7	150	044	154	119	153
8	240	159	253	163	227
9	164	239	166	055	168
10	244	173	037	182	223
11	184	049	185	067	187
12	197	190	089	190	238
13	199	173	202	188	204
14	214	209	191	211	073
15	243	112	129	107	114
16	203	098	122	098	102
17	118	217	172	124	108

As the previous thought, this work again directed towards cross verification of number of bifurcation points. The idea to validate this thought is to ensure if the bifurcation points remains same or varying when the captured retina image is either viewed or obtained at various angles of rotation. Table 4 depicts the bifurcation points as obtained for the same captured and sampled retina image.

Table 4: Comparison of a single bifurcation point with different angles

S.No.	Degree	X	Y	Angle 1	Angle 2	Angle 3
1.	0	185	67	211	73	190
2.	10	192	86	213	96	193
3.	15	195	95	214	106	194
4.	20	197	102	195	119	128
5.	25	199	108	216	121	196
6.	30	202	114	197	129	114

Table 4 infers that when we rotate the image by different angle, the number of end points (EP), bifurcation points (BP) remain same. The above said points remain constant with the change in angular rotation of an image while the angle theta varies with varying rotation.

4.3. Island detection from the thinned image

With the process of detecting end points and bifurcation points for the retina image, the work now focuses towards identification of island which is a closed loop. This paper limits towards the introduction of concept of island without any area specification. Our forthcoming articles will take care of area of boundary regions for the closed loop.

By considering the above used structuring element matrix, whenever the matrix values indicates 1, the inference is that there is a path to travel. Similarly, there may be several such paths in the retina image. However, when travelling via the matrix path, when two paths join at one of the pixel whose value ends with 1 and after which there is no path indicating the pixel values to become 0 infers formation of closed loop.

Figure 5 illustrates the all possible islands formed within the sampled retina image using MATLAB code.

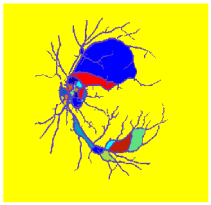

Fig.5. Island image

Figure 5 infers the Number of islands is 34 where there can be island of varying size which is again one more research to progress in order to find the area and using which also to generate keys.

The investigation further confirms that for the sampled image, when rotated with various angles of theta, since the end points and bifurcation points remains same, the number of islands also remain unchanged.

4.4. More Secured key generation using unification of three retina features

The unique contrition of this part of research is to the unification of end points, bifurcation points and island to generate cryptographic key to uniquely identify an individual using retinal biometric approach.

The three feature points are used to generate the key such as the (x, y) coordinate values of each end point, the number of bifurcation points and the number of islands. The algorithm which is applied to generate key using above approach is as follows

EBI Unification Algorithm

Step 1: Read the x and y coordinate values of an endpoint from the thinned image.

Step 2: Compute k_1 using the formula,

$K_1 = \text{Mod}\ (\sum(x[i] * y[i]), p)$.

Where i is the number of end points in an image and p is a prime number.

Step 3: Similarly compute K_2 using bifurcation points

$K_2 = \text{Mod}\ (\sum(x[i] * y[i]), p)$.

Step 4: The number of islands in the image is k3, Fig 5.

Step 5: Cubic polynomial equation, Using curve fitting tool in Mat lab.

$$Key = k_1 x^3 + k_2 x^2 + k_3 x;$$

V. EXPERIMENTAL RESULTS

The above said process of key generation approach is programmed in MATLAB 10 though it still supports MATLAB 12. The work is tested for the proposed approach on retina images. The vascular tree is extracted from the retina image after binarizing. By using the aforementioned three biometric features, the unique cryptographic key is generated.

Since, it is required to validate our work for the collected data in terms of performance evaluation as against the performance with other existing data set, the next step in this research is to prove our concept to be more effective and unique in secured key generation through retinal biometric process. In order to achieve the above objective, experiments are conducted using the same MATLAB code against the data set of VARIA with our collected data set from various medical centers.

Table 5 provides performance matrix on both VARIA and collected data set of medical centers. Table provides details of True Positive Rate (TPR), False Positive Rate (FPR) and accuracy (Acc) for various sampled retinal images. It may be noted here are 100 images for which it is tested with varying threshold values.

Table 5: Performance Matrix on available data set.

Authors	TPR	FPR	Acc
Manual	0.8951	0.0438	0.9473
MARTINEZ(1999)	0.7246	0.0345	0.9344
Hoover (2000)	0.75	0.0438	0.9212
jiang(2003)	0.834	0.0438	0.9212
Stall(2004)	0.678	0.017	0.9441
Montes(2008)	0.593	0.0947	0.918
Fabiola M(2009)	0.921	0.0045	0.99
Tajuddin & C.Nandini (2013)	0.8923	0.003	0.897
Proposed Approach	0.9113	0.005	0.9713

Table 5 infers that when an unauthorized retina image of an individual is used, FPR rate becomes 0 with our approach.

Though the Table 5 indicates only few results, the Figure 7 depicts the performance Matrix values for various thresholds.

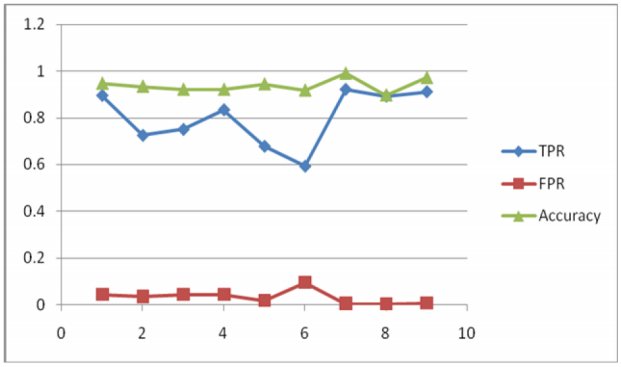

Fig.6. Performance matrix representing TPR, FPR and accuracy.

Figure 6 thus assures with the implementation of unification of three features of retina image to generate key always confirms 0 to non match rates.

It may be recalled that with existing approaches of retinal biometric, there is always a need to pass the generated key to cryptographic application using some cryptographic algorithms. However, with our approach, this need to manually input the key is also eliminated since upon input of image, the key which gets generated automatically moves into the cryptographic algorithm which again entrusts the security of the generated key. The entire process of remembering the generated key and manual intervention is eliminated and the application incorporating this technique itself will take the values of generated key and validates the authenticity of the individual.

This is proven using AES algorithm with three instances as below.

AES Algorithm results

Input Message: 1 2 3 4 5 6 7 8 9 1 2 2 3 4 5 6
cipher : 178 161 167 233 165 95 79 231 3 117 209 66 50 248 178 25

Input Message: 11 22 33 44 55 66 77 88 99 21 22 23 24 25 26 27
Cipher: 233 247 126 177 227 98 29 69 11 123 176 76 213 237 204 206

Input Message: a b c d e f g h i j k l m n p q
Cipher: 234 12 54 187 23 65 87 29 93 102 276 206 129 54 126 201

Applications

With this research, it is now possible for retinal biometric to be applied even in network associated application including cloud based applications.

VI. Conclusion

Securing information across the network is one of the key challenges. Security traditionally was achieved through cryptography approach. However, the recent advent in technology has enabled biometric techniques to generate key to achieve security. Though there exists several biometric modes of ensuring security for cryptographic applications, retinal biometric has all the time taken its significance. Previous work the key is generation by using only one feature that is number of end points and the present work by three features such as end points, bifurcation points and islands.

The aim of this paper is therefore to provide secure way to generate the key using retina biometric features since retina is unique and reduces the probability of duplicates. This research introduces an EBI Unification algorithm that directly generates the unique key from the human biometric information such as retina and is not stored in the database. This approach does not create redundant end points, bifurcation and islands in addition to being more complex in nature to crack or to guess the cryptographic key.

Acknowledgment

The authors would like to sincerely acknowledge the doctors of various medical centers who have provided valuable information of eye, retina and enabled to provide retinal images within the framework of nondisclosure agreement.

References

[1] Manjesh.K.N, R K Karunavathi , " Secured High throughput implementation of AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 , ISSN: 2277 128X.

[2] Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, " Design of AES Algorithm using FPGA," in Universal Association of Computer and Electronics Engineers.

[3] Mg Suresh and Dr.Nataraj.K.R,"Area Optimized and Pipelined FPGA Implementation of AES Encryption and Decryption ," International Journal of Computational Engineering Research Vol. 2 Issue. 7.

[4] M. Nagendra and M. Chandra Sekhar , "Performance Improvement of Advanced Encryption Algorithm using Parallel Computation", International Journal of Software Engineering and Its Applications Vol.8, No.2 (2014),pp.287-296 http://dx.doi.org/10.14257/ijseia.2014.8.2.28 .

[5] C.-F. Lu, Y.-S. Kao, H.-L. Chiang and C.-H. Yang, "Fast implementation of AES cryptographic algorithms in smart cards", Security Technology, Proceedings. IEEE 37th Annual 2003 International Carnahan Conference, (2003), pp. 573-579.

[6] R. Seshadri,T. Raghu Trivedi," Efficient cryptographic generation using biometrics ", IJCT, volume -3 , ISSN- 2229-6093, 2012.

[7] Sanjay Kanade, Dijana Petrovska, Bernadette Dorizzi, "Generation and sharing biometrics based keys for secure cryptographic application", 978-1-4244-7580-3/10/$26.00, 2010 IEEE.

[8] Umut Uladag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, "Biometrics Cryptosystem Issues and Challenges", Proceeding of IEEE, Vol 92, No 5, pp 948 - 960, June 2004.

[9] S. Soutar , D. Roberge , A. Stoianov , R. Gilroy and B.V.K.V. Kumar, " Biometric Encryption ", In R.K. Nichols, editor ICSA Guide to cryptography, pp 649 - 675, McGraw Hill New York 1999.

[10] Literature Review of Cryptography and its Role in Network Security Principles Lloyd Calloway, 8 September 2008.

[11] F. Amin, A. H Jahangir and H. Rasifard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security", World Academy of Science, Engineering and Technology, Vol 17, 2008.

[12] N. Lalithamani , K. P. Sonam, " Imevocable cryptographic key Generation From Fingerprint Template An Enhanced and Effective Scheme", European Journal of Science Research,ISSN-1450-216X, Vol 31 No.3 ,2009, PP 372 - 387.

[13] Rashi Bais, K.K Mehta, "Biometric Parameter Based Cryptographic Key Generation", IJEAT, ISSN: 2249-8958, Vol-1, Issue - 5, June 2012.

[14] 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.

[15] 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.

[16] 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.

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

[18] Daemen, J. and Rijmen, V.: The First 10 Years of Advanced Encryption. In IEEE Security and Privacy, vol. 8, pp. 72-74, November (2010).

[19] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani, "A Novel Cryptographic Key Generation Method Using Image Features**",** Research Journal of Information Technology 4(2): 88-92, 2012, ISSN: 2041-3114

[20] B.Raja Rao, Dr.E.V.V.Krishna Rao, S.V.Rama Rao,M.Rama mohan rao, " Finger Print Parameter Based Cryptographic Key Generation", IJERA ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012, pp.1598-1604

[21] Amrita Sahu,, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for Securing Digital Image" , IJARCSSE, Volume 2, Issue 10,October2012 ISSN: 2277 128X.

[22] C.-S. Laih, and K. Y. Chen, "Generating visible RSA public keys for PKI", International Journal of Information Security, Vol. 2, No. 2, Springer-Verlag, Berlin, 2004, pp. 103-109.

[23] Theodore S Rappaport " Wireless communications" principle and practice 2nd Edition.

[24] Ravi Das, "Retina Recognition", Biometric technology in practice, keesing journal of document and identity, issue 22, 2012.

[25] Gunjan Gupta and Rama Chawla, " Review on Encryption Ciphers of Cryptography in Network Security", IJARCSSE,volume 2, issue 7, July 2012, ISSN2277 128X.

[26] Ogiela M.R and Ogiela .L " Image Based Crypto-biometric Key Generation", Intelligent Networking and Collaborative Systems (INCoS), hird International Conference on IEEE 2011**.**

[27] Digital image processing by Gonzalez, 3rd Edition.