Key Creation Using Biocryptosystem To Secure The User Data In Cloud Environment

M. Akila , Dr.S.Ravichandran

Abstracts: his paper deals the generation of biometric keys for the cryptosystem and furthermore, the significant skeptic of the users is that "Is our entire data safe and secured?" and to earn the trust of the users the biometric security is utilized while movingthe user data to and from the cloud archives. The paper deals with fingerprint security and begins from acquiring the fingerprint from the client, preprocess the fingerprints to enhance the clarity, extricate the significant features, convert the features into bit matrix structure, and create large number of keys for a specific user from the biometric procured from them. The greater part of the users faces tremendous trouble to remember long and complex cryptographic keys and hence the key is generated from the biometric procured from them. The principle goal of this paper is to incorporate the fingerprint of the client to deliver the security key to be utilized in cryptosystem particularly in the cloud storage.

Keywords: Biometric, Cloud security, Crypto keys, Fingerprints, Minutiae, SecurityThe User Data In Cloud Environment

1. INTRODUCTION

The unimaginable development and the advancing idea of the PC innovations firmly stress the importance of a dependable security mechanism to conquer the tangles and the limitations present in the current security approaches. The majority of the security systems discovered today are of not versatile enough (can be broken or stolen) to avoid hacking and poached quite easily because of the superior techniques pursued by the hackers. Biometrics has risen basically as a better alternative and intends to serve and fill the security lapses than customary password techniques used today. Biometrics which deals with the examination of seeing a person on the reason her/his physiological or direct ascribes has started to achieve a veritable methodology for perceiving a client's unique identity. The cloud computing offersabundant storage space to plethora of users across the globe and this technology is fundamentally centered on open system and platforms developedmainly to satisfy the secured storage need of the consumers. These storage systems require the top security to ensure tamper free data transfer and grasp the trustworthiness of the clients.Hence cryptography and biometric plays a pivotal role in cloud environment to protect the user's precious data.Lot ofresearches related to cloud security are carried out to fuse the cryptosystem and the biometric to enhance the overall security and this paper presents a novel method to create encryption key from the features extracted in the fingerprints. The important biometric features currently being employed by the research scholars are fingerprint, iris, retina, face, gait, palm-vein pattern, signature, and speechaccording to the author [M.Baca et al., (2005)].

RELATEDWORKS

Of lateplethora of researches and developments related to cryptographic key generation from biometric features and securing the user data by fusing these two has emerged as an important research work and some of the previous works are examined here in this section.

- *M.Akila ,Research Scholar, PG and Research Department of Computer Science,H.H The Rajah's College(A), Pudukkottai.E-mail:vaakila260101@gmail.com*
- *Dr. S. Ravichandran, Assistant Professor and Head,*
- *PG and Research Department of Computer Science,*
- *H.H The Rajah's College(A), Pudukkottai. Email:rajahsravis@gmail.com*

The author [FengHao et al., (2005)] proposed a cryptosystem key based on the user iris features which is capable to produce 99% error free keys with hundred percent success rates. This author used the technique with 140 features that are good enough to produce 128 bit AES. The author [Beng.A et al., (2008)]proposed a biometric-key generation approachwith the aid of the biometric helper whichuses the principle of code redundancy construction while generating the keys and this support the intra class variation of biometric data to the highest level. The author [Muhammad Khurramet al.,(2008)] developed an intelligent multimodal face and fingerprint biometrics security system on the smart cards, driver license, and Identity card. The Fingerprint templates were encrypted and embedded within facial images present in the card and hence the important characteristics present in the fingerprints does not get damaged and corrupted when the process of encoding and decoding occurs. The author [Gang Zheng et al.,(2006)] produced a new technique created with lattice mapping based on fuzzy for the key generation from biometric features. This methodactually concealed the original biometric data from the intruders and also produced high security keys.

BASIC IDEA

The inspiration of this research paper depends on the perception that for every single security task, an altered security component is needed and after analyzing many research works identified with biometric security and finding the confinements, deficits and glitches present, the idea of utilizing the fingerprints to create the cryptographic key is planned. The security breaches prevailing over the globe with the regularly advancing technology and the expansion in the quantity of hacking assaults on the precious data transmitted over the cloud condition pervades and inspires a lot of specialists to build up various techniques to overcome the security related issues.

FINGERPRINTS

A fingerprint is a unique entity full of edges and wrinkles on the base surface of the fingers. Every single individual have a unique fingerprint and no two fingerprints has a similar regular features. The uniqueness of the fingerprint is dictated by the nearby edge features and their relationship. So far more than 150 numbers of local ridge features are

recognized and these features exactly rely upon the fingerprint and the nature of the image captured by the device. The two most significant edge features, called details, are (1) edge ending – the point where the edge closes suddenly (2) edge bifurcation – the point where an edge separates into branch edges. Commonly a decent quality fingerprint contains somewhere around 40 to 100 unique features. A run of the mill unique finger impression with edges is shown in the figure 1.

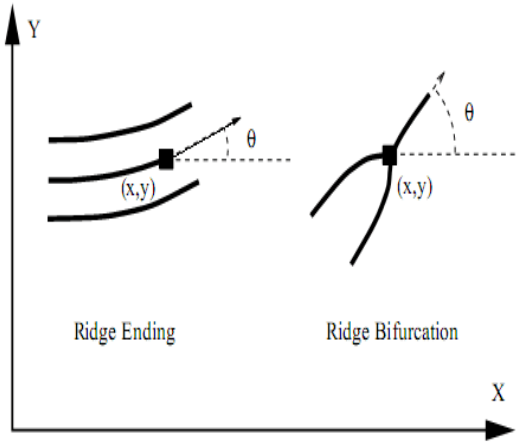

Figure 1: *Sample ridges in the fingerprints*

PROPOSED APPROACH

The proposed approach comprises of many stages as shown here under,

1. Enhance the quality of the Fingerprint
2. Acquiring the minutiae points
3. Creation of binary matrix
4. Generate the final Key

ENHANCE THE QUALITY OF THE FINGERPRINT

The quality up gradation of the fingerprint procedure includes lot of work as the nature of the fingerprints plays a pivotal job in the extraction of the important features from the fingerprints. At first the input fingerprint is taken, and the fingerprint is standardized to discover the predefined mean and difference present in it. The direction of the picture is assessed from the standardized image and estimated to correct the orientation. To check whether the fingerprint areas can be ordered into recoverable and non-recoverable obstructs, the region mask estimation is done and the filtering process is applied to increase the quality of the fingerprint as shown
in the figure 2.

Figure 2: *Quality enhancement of the fingerprint*

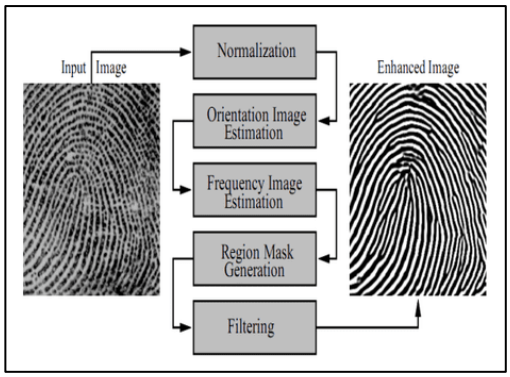

Figure 3: *Input image, Normalized image, Orientation estimated image*

ACQUIRING THE MINUTIAE POINTS

The quality improved fingerprint picture is then used for the methodology of minutiae point extraction. To complete the extraction methodology, we at first apply the binarization and morphological exercises to the improved unique fingerprint picture. Binarization is the strategy for changing the gray level picture into a binary image. Morphological errands are used to remove pointless spikes, bridges and line breaks are cleared. The edge diminishing count is used for removing the dreary pixels till the ridges end up one pixel wide. Starting there ahead, minutiae centers are isolated from the reduced unique mark picture. The genuine minutia features of unique finger impression ridges are: edge endings (the unforeseen finish of an edge), bifurcation (a single edge that branches into two ridges).

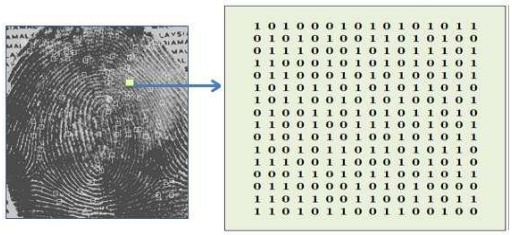

Figure 4: *a) Input image b) Enhanced image c) orientation estimated d) minutiae extracted*

CONVERT TO BINARY MATRIX

Once the minutiae points are found the key generation process starts and the minutiae area is extracted as a 16 x 16 bit matrix to generate the key as shown in the figure 5.

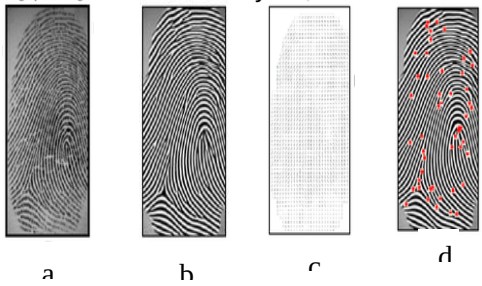

Figure 5*: Conversion of minutiae point into binary matrix*

The 16 x 16 binary matrix shown in the figure 5 is grouped into 4 x 4 binary matrix starting from left most top and then towards the right and then down to perform key generation operation.

GENERATE THE FINAL KEY

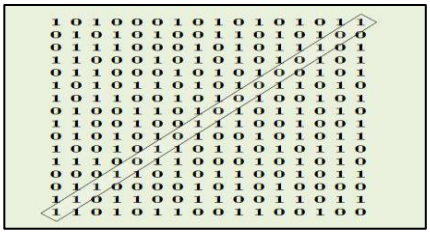

Figure 6: *The minor diagonal value fetched from binary matrix*

The next important process is to fetch the minor diagonal values from the binary matrix as shown in the figure 6 and then the fetched binary values are converted into decimal value.

The fetched minor diagonal value 1010000010101111 is taken and NOT operation is applied to get the value 0101111101010000 and this binary value is converted into a decimal value as shown below

Decimal value D = 24400

The value of D is divided by 16 to get the common key value C as shown below

Common Key C = 24400 / 16 => 1525 ---------- Equation (1)

This value generated is used during the process of key generation and illustrated in the following section. Now the binary matrix shown in the figure 5 is sub-divided into sixteen 4 X 4 matrix and the sub division is shown in the figure 7. The binary values present in the sixteen 4 X 4 matrix is fetched to generate a decimal matrix comprising of 16 values (4 X 4 decimal matrix).

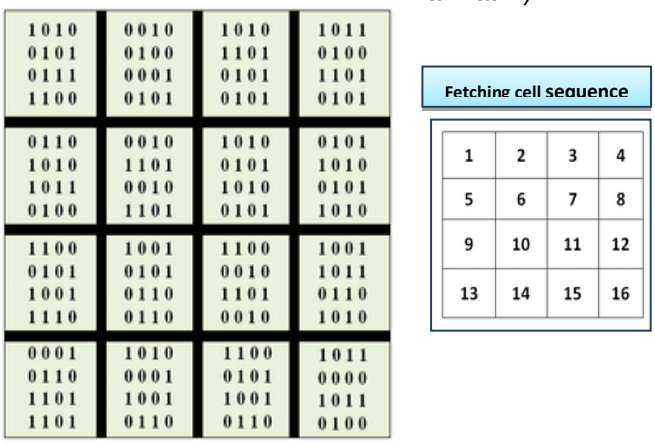

Figure 7: *Sixteen (4 X 4)matrixes and the order in which the matrix are fetched*

The figure 7 showcases the sequence in which the 4 X 4 matrixes has to be retrieved to generate the keys. The first cell values are retrieved and then the binary values present in the 4 X 4 matrix cell are fetched as shown in the figure 8 along with the pattern in which the binary data is retrieved.

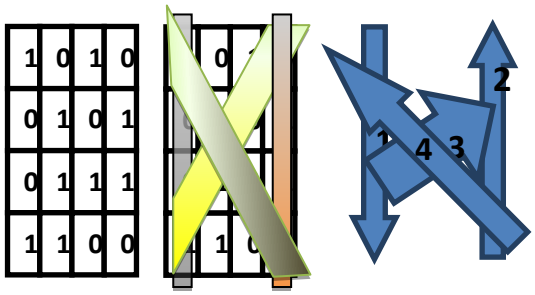

Figure 8: *Data fetching mechanism from the first 4 X 4 matrix*

The data fetched from the cell 1 of the 16 cells present in the figure 7 is shown in the figure 8 and the pattern used to retrieve the binary values is also shown. The detailed binary values obtained are clearly enumerated in the figure 9.

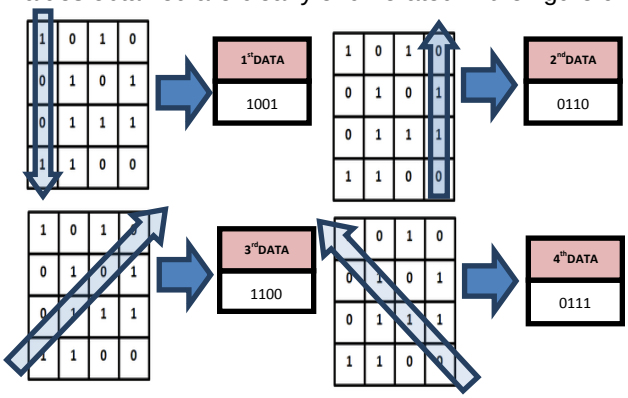

Figure 9: *Actual process in the extraction of binary data*

The figure 9 extracts the binary data from the cell number 1 of the figure 7 and the data fetched is [1001][0110][0111][1100] and these binary digits are concatenated to get 1001011001111100 which is then converted into decimal values. Decimal of [1001011001111100] = 38524This decimal value fetched from the first cell in divided by the common key found in the equation 1. Calculation is 38524 / C => 38524 / 1525 → 25.261639 (rounded to six digits) and similarly all the cell values are extracted using the pattern shown in the figure 9 and then divided by the common key, round the value to six digits, to get the resultant value. The resultant decimal matrix formed from the single minutiae is shown in the figure 10 and as illustrated earlier every good fingerprint image comprises of more than 100 minutiae points, it is possible to create many number of keys for one fingerprint based on one pattern as shown in the figure 9.

Table 1: *Decimal values extracted from one minutiae point*

25.261639	0.608524	33.523934	28.824262
16.494426	14.420983	27.687868	15.118032
30.588852	45.006557	27.150163	36.972459
10.019016	27.876721	27.897704	28.590819

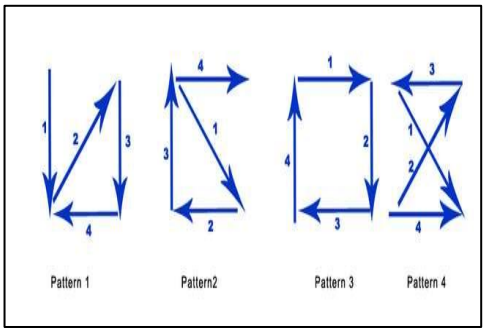

Figure 10: *Decimal equivalent of a single feature present in the fingerprint*

Here the data from the matrix shown in the figure 10 is retrieved in the similar fashion as shown in the figure 9 but the whole numbers and the fractional parts are separately concatenated as shown in the following illustration,
First Data [25.261639][0.608524][33.523934] [28.824262]
Here the whole numbers 10 0 12 20 are concatenated separately and 280854 005933 951740 01384 are concatenated separately to get,
= [2503328][26163960852452393482426]
Similarly all the data from the figure 10 is fetched and concatenated as shown.
Second data [16.494426][14.420983][27.687868] [15.118032]
= [16142715][49442642098368786811803 2]
Third data [30.588852][45.006557][27.150163] [36.972459]
= [30452736][58885200655715016397245 9]
Fourth data[10.019016][27.876721][27.897704] [28.590819]
= [10272728][01901687672189770459081 9]

The resultant values are shown in the table 1 and the keys are formed from these rows and columns as shown in the following illustration.

Table 1: Decimal values extracted from one minutiae point

Here the values in the first columns is initially taken and concatenated and then the values in the second column are procured to concatenate and the results are concatenated to form the encryption key.

First column value = 25033281614271530452736102727 28
Second column = 26163960852452393482426249442642098368786811803 2 58885200655715016397245 9 01687672189770459081 9

The final encryption key = 25033281614271530452736102727282616396085245239 34824262494426420983687868118032588852006557150 163972459 01687672189770459081 9

The final key can be utilized in the cryptographic algorithm to safe guard the data during the transfer from the user end to the cloud storage. The final key is generated using one pattern in the shape of “11X” and numerous keys can be generated using different patterns while fetching the data is shown in the figure 11. As the number of patterns increases the corresponding number of keys generated will also increase and thousands of keys are generated for a particular user and archived to be utilized when the data transmission takes place between the user and the cloud storage.

Decimal values extracted from one minutiae	
2503328	261639608524523934824262
16142715	494426420983687868118032
30452736	588852006557150163972459
10272728	01687672189770459081 9

Figure 11: *Various patterns that can be used to retrieve the 4 X 4 matrix data*

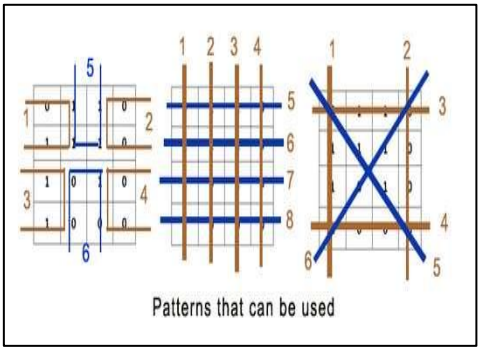

Figure 12: *patterns that can be used*

Similarly to increase the length of the keys the patterns can be increased as shown in the figure 12. to retrieve binary data from matrix

EXPERIMENTAL RESULTS

The experiment is conducted acquiring fingerprint images from FVC database http://bias.csr.unibo.it/fvc2000/and the hardware used is a system with I3 Pentium processor with 4GB RAM and the codes are written using java and the keys generated are stored as a simple flat file (Note this keys can be stored in separate key security files for safety). The number of keys discovered from a fingerprint depends on the number of the minutiae points, number of patterns used and it is up to the user to decide the volume and the size of the key to be produced. Longer the size of the keys, it is quite difficult to crack and break, the keys obtained from two or more minutiae points can be combined to form a very lengthy key.

KEY GENERATION ALGORITHM

Algorithm CreateBiometricKeys(Input Image, Scheme S)
Input: Fingerprint F and Scheme S Output: biometric key Begin: 1. Load the input fingerprint and carry preprocessing 2. Improve the image quality 3. Fetch the minutiae points FP 4. For each minutiaePoints fmP in FP do begin 5. Convert fmP →Binary matrix format 6. Extract the minor diagonal values in the binary matrix 7. Apply NOT operation and convert the value to decimal 8. Compute the commonkey C=Decimal/16 9. Subdivide the matrix into 16 [4 X 4] matrixes. 10. Apply the scheme S to fetch the binary values 11. Convert the binary values to decimal 12. Divide the resultant by the commonkey C 13. Concatenate the values of whole numbers and fraction parts separately and then combine both values to get the final key. 14. StoreFinal Key→ K 15. Next For 16. Return Final Keys K End

Figure 13: *Pseudo code of CreateBiometrickeys algorithm*

CONCLUSION

This paper showcases different key generation schemes that can be produced from the fingerprints of the users that can be utilized the cryptosystem for encryption/decryption to safe guard the data in the cloud environment. These keys generated are very large and can be utilized in any cryptographic algorithm toprotect the user data from the intruders and hackers. Since thousands of keys are generated from one user fingerprint, the key repetition for encryption/decryption can be avoided and makes it harder for the intruders to breach and more importantly the tedious process of remembering the long passwords and passcodes for the users are evaded.

REFERENCES

[1] M Baca and K. Rabuzin, “Biometrics in Network Security”, in Proceedings of the XXVIII International Convention MIPRO 2005, pp. 205-210 , Rijeka,2005.

[2] Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometrickey generation with biometric helper”, in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications, pp.2145-2150, Singapore, June 2008.

[3] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces", in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007

[4] Christian Rathgeb, Andreas Uh, “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP Journal on Information Security 2011.

[5] FengHao, Ross Anderson, John Daugman, (2005) “Combining cryptography with biometrics effectively”, Technical Report No. 640, UCAM-CL-TR-640, ISSN 1476-2986.

[6] Gang Zheng, Wanqing Li and Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping", in Proceedings of the 18th InternationalConference on Pattern Recognition, vol.4, pp. 513 - 516,2006.

[7] Jagadeesan.A, T. Thillaikkarasi, K. Duraiswamy, “Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature”, International Journal of Computer Applications (0975 – 8887) Vol. 2 – No.6, pp. 16-26, June 2010

[8] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026-3031, August 2008.

[9] S. Vitabile, V. Conti, M. Collotta, G. Scatà, S. Andolina, A. Gentile, F. Sorbello, "A Real-Time Network Architecture for Biometric Data Delivery in Ambient Intelligent", Journal of Ambient Intelligence and Humanized Computing (AIHC), (in press), © Springer-Verlag Editor, 2012

[10] SP.Venkatachalam, P.MuthuKannan, V.Palanisamy, “Combining Cryptography with Biometrics for Enhanced Security”, International Conference on Control, Automation, Communication and Energy Conservation, INCACEC 2009, pp. 1-6, ISBN: 978-1-4244-4789-3