- Selecting an integer *e* that is relatively prime to $\varphi(n)$. (i.e. the greatest common divisor of *e* and $\varphi(n)$ *is* 1)
- Selecting two numbers *a* and *b* such that *b* = *a* * *e*.
- A pair of public keys are then generated {*b*, *n*}, {*a*}.
- Calculate the value *d* as multiplicative inverse of *e* modulo $\varphi(n)$.
- To calculate *d* the receiver chooses a positive natural number and multiply it with *a* and then add *b*. Divide the result by *a* and finally subtract the chosen value. Then the receiver will have *e*. Then calculate *d* as usual.
- The value *e* and *d* will have the desired properties of values in RSA.
- If user Q want to send data to P, then user Q must calculate $C = M^{b/a} \bmod n$ and transmit the data C to P.
- Then user P receives the encrypted data and decrypted to get the data M by calculating the value $M = C^d \bmod n$.

4. Proposed Data Protection Method

The proposed data protection method contains various processes such as enrollment of two different fingerprints, creation of a virtual identity using these two fingerprint images, authentication of the fingerprint is done to verify the user. A modified RSA cryptosystem is used to encrypt and decrypt the user data.

4.1 Enrollment of Fingerprints

In the enrollment phase the user need to use two different fingerprints to create the virtual fingerprint identity. Once the two different fingerprints are enrolled in to the system, the system then creates a virtual fingerprint identity and stores them to the system server or wherever the virtual identity is intended to be saved.

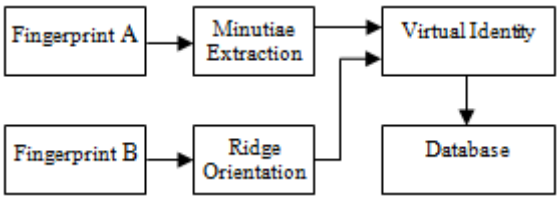

Figure 6: Enrollment of fingerprints

4.2 Authentication of Fingerprints

In the authentication phase the same two fingers of the user which were used for the enrollment process are used as the query fingerprints. A virtual identity is created from the query fingerprint images. Minutiae positions from the first fingerprint and the ridge orientation is taken from the other fingerprint. Then the generated query fingerprint template is matched with the virtual identity template in stored in the database. If the similarity is greater than a threshold value the user gets the authentication to do the remaining processes.

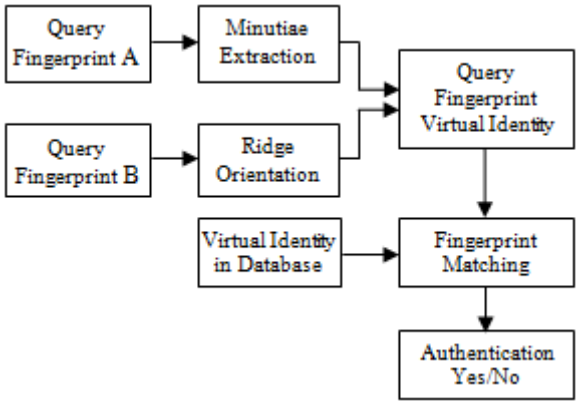

Figure 7: Authentication of fingerprints

4.3 Cryptographic Data Protection

In the proposed data protection method a modified RSA cryptosystem is used for the encryption and decryption of the user data. Here a text message is used as a secret user data. In order to do the encryption the modified RSA need two prime numbers to generate the private key and the public key. Here in the proposed system there are two public keys i.e. a pair of public keys are used for encryption process. These keys are sent to the sender over a secure transmission medium in order to encrypt the data. The prime numbers are selected in such way that they will be unique for each and every individual user and is obtained from their virtual identity. This is the main advantage of this system. Upon receiving the encrypted data the user can decrypt it using the private key.

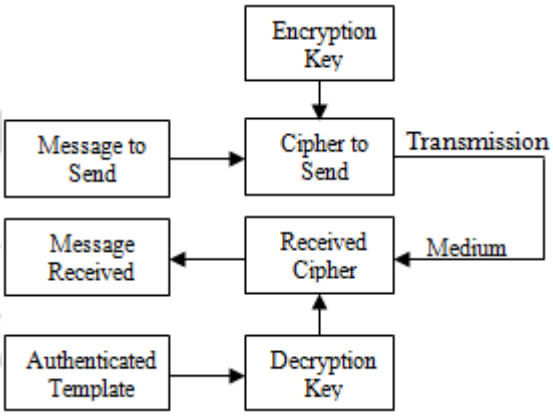

Figure 8: Proposed data protection method

5. Acknowledgement

Authors are obediently thankful to God Almighty, praise and glory is to Him, for all His uncountable bounties and guidance, without which, this work would have never been a reality. The authors would like to thank all the faculties in E.C.E. department in MEA Engineering College for all their support during the work. Also authors like to thank all unknown referees whose papers helped during this work.

6. Future Scope

This data protection can be used to encrypt and decrypt secret data which are in the form of images. This can also be used to protect private videos any other type of data. In this paper the protection of a secret text message is only

described. . In order to protect the user images and videos appropriate methods can be used. This method can be used for any other type of user data.

7. Conclusion

In this paper a new approach for the data protection is introduced. The data protection is carried out using the virtual biometric identity of the user and a modified RSA cryptosystem. Using two different fingerprints and combining them in a certain way to create a new virtual identity by generating an integrated template. Minutiae positions are taken from one fingerprint and orientation is taken from the other. We then make a unique alternation to the integrated template and then stored in the database. Thus a new identity is created and makes it more secure in case of a theft. Since the fingerprints are randomly chosen and because of the altering to the integrated template we will be able to create a better new virtual identity. From the virtual identity a pair of keys are generated which then used with modified RSA cryptosystem to provide encryption and decryption for the user private data. This can only be done after verifying the user by matching the virtual identity created from the query fingerprint virtual template and the virtual fingerprint identity stored in the database.

References

[1] Sheng Li and Alex C. Kot, "Fingerprint Combination for Privacy Protection", IEEE Trans. Inf. Forensics and Security, vol. 8, no. 2, Feb. 2013.
[2] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An Analysis of Biohashing and its Variants," Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006.
[3] N.K.Ratha, S.Chikkerur, J.H.Connell, and R.M.Bolle, "Generating Cancelable Fingerprint Templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.
[4] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
[5] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-Biometric Templates Using Fingerprint and Voice," Proc. Spie, vol. 69440i, pp. 69440i-1–69440i-9, 2008.
[6] Y. Wang and J. Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 1, pp. 72–87, Jan. 2011.
[7] J. Feng and A. K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp. 209–223, Feb. 2011.
[8] Li and A. C. Kot, "Privacy Protection of Fingerprint Database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.
[9] A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.
[10] S. Li and A. C. Kot, "Attack Using Reconstructed Fingerprint," Inproc. IEEE Int. Workshop On Inform. Forensics and Security (Wifs), Foz Do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
[11] A. Othman And A. Ross, "Mixing Fingerprints for Generating Virtual Identities," Inproc. IEEE Int. Workshop On Inform. Forensics and Security (Wifs), Foz Do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

Author Profiles

Rishin Ali K received B.Tech degree in Electronics and Communication Engineering from MES College of Engineering, University of Calicut, Kerala, India in 2010. Then he worked for Tata Teleservices Ltd., Kerala circle in 2010 for implementing Mobile Number Portability (MNP) in India. After that he completed advanced diploma in Embedded Systems from Cranes Software International during 2011 and 2012. Currently he is doing M.Tech in Communication Engineering from University of Calicut.

Mohammed Aslam V.N received B.E degree in Electronics and Communication Engineering from SNS College of Engineering and Technology, Anna University, TamilNadu in 2006. He received his M.E in Communication Systems from SriKrishna College of Engineering and Technology, Anna University, Coimbatore, TamilNadu in 2009. Currently he is working as Assistant Professor in the Department of Electronics and Communication in MEA Engineering College, Perinthalmanna, Kerala.