International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data Protection Using Virtual Identity and Modified RSA

Rishin Ali K[1], Mohammed Aslam V.N[2]

[1]Dept. of ECE, MEA Engineering College, University of Calicut, Perinthalmanna, Malappuram, Kerala, India - 679325

[2]Assistant Professor, Dept. of ECE, MEA Engineering College, Perinthalmanna, Malappuram, Kerala

Abstract: ***This is a new system for protecting user data using integrated fingerprint template, virtual identity and modified RSA. In the process of fingerprint enrolment, two different fingerprints are used. The minutiae positions from one fingerprint, orientation from the other one and reference points from both fingers are used. Using unique coding technique an integrated minutiae template is generated from these two different fingerprints and stored in the database. This makes it more secure in case of a theft, it will be difficult for the attacker to distinguish the integrated template from the original template since their topology is similar. In the authentication process, system requires two query fingerprints from the same fingers which are used for the enrolment. Multi-stage fingerprint matching is proposed for matching the query fingerprints with the integrated minutiae template. We are selecting the fingerprints randomly and because of the altering to the integrated template we will be able to create a better new virtual identity. Features of the generated virtual identity is used to implement the modified RSA algorithm for the data protection. We can make the data protection technique unique for each and every user since the encryption and decryption of data is done using their fingerprint identity. This technique can be used for protecting various user data.***

Keywords: Data protection, Fingerprint, Virtual identity, Modified RSA, Cryptography.

1. Introduction

A virtual fingerprint identity is created using two different fingers of the user. This virtual identity is used for the protection of the secret data. The advantage of using virtual identity is that in case of an attack to the data server that is used for saving the fingerprint, the identity of the user is not compromised. The attacker will not understand the virtual identity and the regenerated fingerprint will not have any similarity to the original user fingerprint. Fingerprint techniques is widely used in the authentication processes. So protecting the privacy of the fingerprint is an important issue. Traditional encryption of the fingerprint image is not sufficient for privacy protection because decryption is required before the fingerprint matching. This exposes the fingerprint to the attacker. Some of the existing techniques make use of a secure key for the fingerprint privacy protection. They may also be vulnerable when both the key and the protected fingerprint are stolen. Some are able to protect the privacy of the fingerprint without using a key. Some of them uses visual cryptography for protecting the privacy of biometrics. They produce two noise-like images (sheets) from a single fingerprint image which are then stored in two separate databases. A single image cannot reproduce the property of original image. The two images must be available simultaneously. It requires two separate databases to work together, which is not practical in some applications. Some privacy protection technique make use of the voice of the user to create fake minutiae which is then integrated into the minutiae created from the fingerprint image. Thus it is difficult for the attacker to distinguish the fake and real minutiae in order to reconstruct the original fingerprint template. The concept of integrating multiple fingerprints into a new identity is then proposed. Using this integrated virtual identity fingerprint template we can extract some unique feature that is distinct for each individual to introduce a new encryption and decryption method.

2. Virtual Fingerprint Identity

To construct the virtual fingerprint identity the user need two different fingerprint, one for minutiae extraction and another for ridge orientation extraction.

2.1 Minutiae Points Extraction

Minutiae points are extracted using some existing methods [1]. The fingerprint image is first selected and processed in order to extract the minutiae points. The image is first enhanced to get the clear view of the fingerprint ridges. Some fingerprint images might be very poor in quality to extract the minutiae points. These images must be processed to enhance the distinguishability of the ridge patterns. Then only the minutiae can be extracted accurately. Enhancement of the fingerprint image uses some existing techniques, which produces a much more clear view of the ridges. Then the enhanced image ridges are thinned into one pixel width. This process uses the inbuilt functionality of the Matlab. Then a sliding window technique is used to find out the minutiae points in the fingerprint. A 3x3 sliding window slides across the fingerprint image to find out the ridge endings and the ridge bifurcation. By using this technique we will get the exact coordinates of the minutia point location.

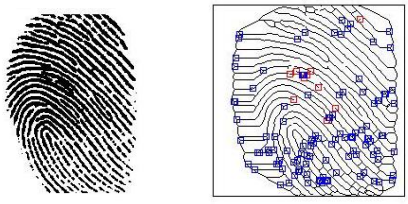

Figure 1: Fingerprint A and minutiae points

2.2 Ridge Orientation Extraction

Ridge orientations are needed to complete the unique property of a fingerprint. A least mean square orientation estimation algorithm [6] is used to find out the ridge orientation of the given fingerprint image. The principal axis of variation in the image gradient is found out by using a Gaussian filter. The normalized image is first divide into 16x16 block size. Then image gradient at each pixel (i,j), $\partial_x(i,j)$ and $\partial_y(i,j)$ are computed. The local orientation of each block at pixel (i,j) are then estimated. This gives the direction that is orthogonal to the dominant direction of the Fourier spectrum of the *w* x *w* window. Due to the presence of noise, corrupted ridges and minutiae the estimated ridge orientation may not always be correct. A low pass filter can be used to correct the incorrect ridge orientation. The orientation image is converted to *continuous vector field* to perform the low pass filtering. The local ridge orientation at (i,j) are calculated using the equation

$$\theta(i,j) = \frac{1}{2}\tan\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right)$$

A fairly accurate ridge orientation can be obtained using this method.

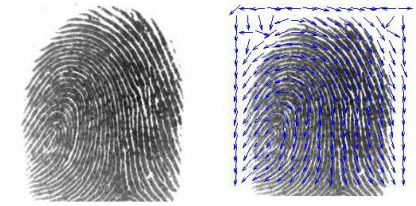

Figure 2: Fingerprint B and ridge orientation

2.3 Reference Point Detection

In order to match two fingerprint we need landmark point which are less prone to misidentification. These points have certain distinct features which makes them easily identifiable by humans. These points can be otherwise called as singular points [6] and can be identified by its symmetry properties. They can be identified by their strong response to complex filters designed for symmetry extraction. In order to find out the singular points we are using two different filters, one for the "core type" and one for the "delta type" symmetry.

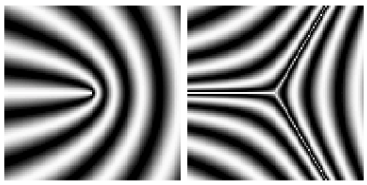

Figure 3: Core and Delta pattern in a fingerprint

Using complex filters to identify the reference point has the advantage to extract the position and the spatial orientation. When the two fingerprint images are rotated and translated relative to each other this method can estimate both rotation and transition parameters at once. A Gaussian is used as the filter window because the Gaussian is the only function which is orientation isotropic (function of radius only in polar coordinates) and separable. These filters are not applied to the original fingerprint image but applied to complex valued orientation tensor field image $z(x,y) = (+if_y)^2$ where f_x the derivative of original image in x-direction is and f_y is the derivative in y-direction. The filters of first order symmetry or parabolic symmetry is used i.e.

$$h_1(x,y) = (x+iy)g(x,y) = r\exp\{i\varphi\}g(x,y)$$
$$h_2(x,y) = (x-iy)g(x,y) = r\exp\{-i\varphi\}g(x,y)$$

The pattern that have local orientation description of $z = \exp\{i\varphi\}$ is similar to core and $z = \exp\{-i\varphi\}$ is similar to delta. So this technique can be used as reference point extractor.

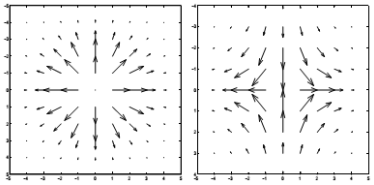

Figure 4: Filter h_1 and filter h_2

Filter h_1 is used to detect "core type" symmetry and filter h_2 is used to detect the "delta type" symmetry.

Figure 5: Reference points of Fingerprint A and B

3. Modified RSA Cryptosystem

RSA is a block cipher and the plain text and cipher text are integers from 1 to *n*-1 for some n. The encryption and decryption can be expressed as follows for plain text M and cipher text C.

$$C = M^{b/a} \bmod n$$
$$M = C^d \bmod n = (M^{b/a})^d \bmod n = M^{b/ad} \bmod n$$

Both sender and receiver knows the values of *n*, *a*, *b* but the value of *d* is only known to the receiver. The public key of this method is having a pair of key *PUK* = {*n*, *b*}, {*a*} and a private key *PRK* = {*d*, *n*}.

Table 1: Advantages of modified RSA

RSA	Modified RSA
RSA uses single pubic key	Uses a pair of public keys
Communication overload is less	Communication overload is high
More vulnerable to brute force attack	Less vulnerable to brute force attack
Comparatively less secure	Comparatively more secure
Pubic key is sent once	Public key is send twice separately

3.1 Steps of Encryption and Decryption

- Two prime numbers *p* and *q* are selected. Their product *n* is then calculated.
- The value $\varphi(n)$ referred to as the *Euler totient* of *n* which is relatively prime to *n*.

- 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.

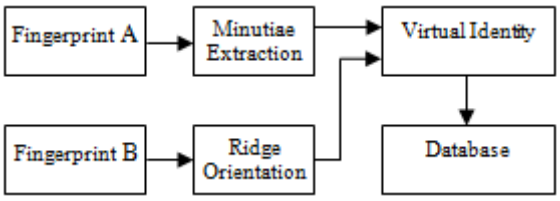

Figure 6: Enrollment of fingerprints

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.

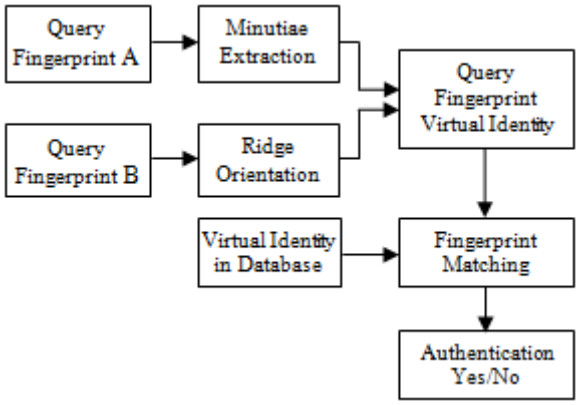

Figure 7: Authentication of fingerprints

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.

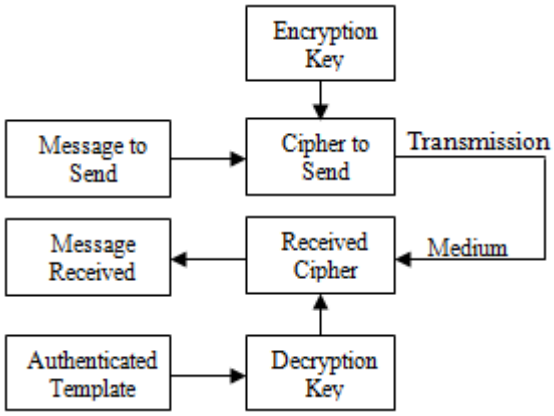

Figure 8: Proposed data protection method

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.