Two Factor Biometric Key for Secure Wireless Networks

P.Muthu Kannan,
Associate Professor, School of Electronics Engineering,
VIT University,
Vellore, India.

V.Palanisamy
Associate Prof. & Head i/c, Department of CSE,
Alagappa University,
Karaikudi, India.

***Abstract*-The applications of wireless networks is steadily increasing through out the world. Wireless transactions are now happening in highly secure banking networks. To have more reliable networks, security of wireless networks is to be strengthened. Various Encryption algorithms are employed for this purpose. With standard key size and format, they are vulnerable to attacks. A key generated from biometric feature is unique and it is hard to break it. If the biometric key is based on key generated from two biometric features, it is highly reliable. In this paper, one such attempt is made to generate key for standard encryption algorithm from keys generated from face and fingerprint with the application of a unique algorithm.**

Keywords – Biometric, Face, Fingerprint, Two factor Biometric key, Wireless Networks.

I.INTRODUCTION

The world has been witnessing lot of wireless applications. The wireless networks are easy to handle and convenient to move. It has its own limitations also. They are battery lifetime and the security of the network. The security aspect needs lot of concern as a breach in security may lead into loss of privacy and wealth as even bank transactions are executed with wireless networks nowadays. The security requirement is to be of very high level. Conventional encryption algorithms are employed for this purpose. These algorithms use encryption keys, of 128 bit or more. The key management is the weakest point of any cryptosystem, as it can be guessed, found with a brute force search, or stolen by an attacker.[3]

To overcome these problems, key generated from biometric can be used. Biometric of a person presents unique characteristics. Uniqueness of the biometric results unique biometric key which is used with conventional encryption systems. Biometrics is based on unique personal features, such as a subject's voice, fingerprint, or iris. It has the potential to identify individuals with a high degree of assurance, thus providing a foundation for trust. A strong combination of biometrics and cryptography has the potential to link a user with a high level of assurance [4]. Even though, an intruder can manage to get data due to sniffing, it is not possible for him to know the biometric key. Though this system has some limitations such as copying of biometric images, it is a highly reliable system. To provide more security level for this system, two factor biometric key can be used. This is generated from the key generated from more than one biometric. In this paper, the keys from 'face' and 'fingerprint' biometric are used to generate two factor biometric key using specific algorithm. This can provide reliable biometric key for encryption algorithms and can be used in wireless networks for better security.

II. THE PROBLEM

The key for a cryptographic system should maintain its secrecy and it should be reliable. This holds the security of any system. In the case of wireless networks, intruders from outside can also get the data as they can get the signal transmitted from an access point [AP]. As the data packets can be sniffed quite easily, the security of the network is at the brink if the key of the encryption algorithm can be broken.

There is a requirement of a 'key', which can not found out even though the data can be sniffed by the intruder. As biometric provides uniqueness in the data, it is highly reliable to be used as a 'key' for the encryption algorithms.

Presenting fake biometrics, tampering with the biometric feature presentation, attacking the channel between stored template and the matching unit, corrupting the matching unit are few possible attacks that can be carried out by the intruders on the biometric key authentication process.
To avoid the above mentioned attacks, two factor authentication biometric key can be used. In this method, biometric key is generated from two biometric features. The biometric key is generated using those two keys with certain algorithm which should be very good against the attacks. The algorithm with which the biometric key is generated is discussed in this paper.

III. BIOMETRIC KEY GENERATION FROM FINGER PRINT

Finger prints are used for personal identification for centuries together. Even now, it is extensively used in the Police Department to identify culprits. The matching accuracy of finger print is very high. The finger print consists of number of ridges and valleys. Ridges are upper skin layer segments and valleys are lower segments. There are two algorithms generally used to match the finger prints: Minutiae matching and Pattern matching. Pattern matching compares overall characteristics of the finger prints. Minutiae matching compare specific details on the ridges. At the matching stage, the minutiae points are extracted from finger print images. Minutiae matching are discussed in this paper. The major steps involved in minutiae matching are segmentation, orientation, image enhancement and minutiae extraction [5]. The minutiae extraction is the important process which involves binarization and morphological operations. The cryptographic key is generated from the extracted minutiae points. The sample finger print and the biometric key generated from that sample are given below.

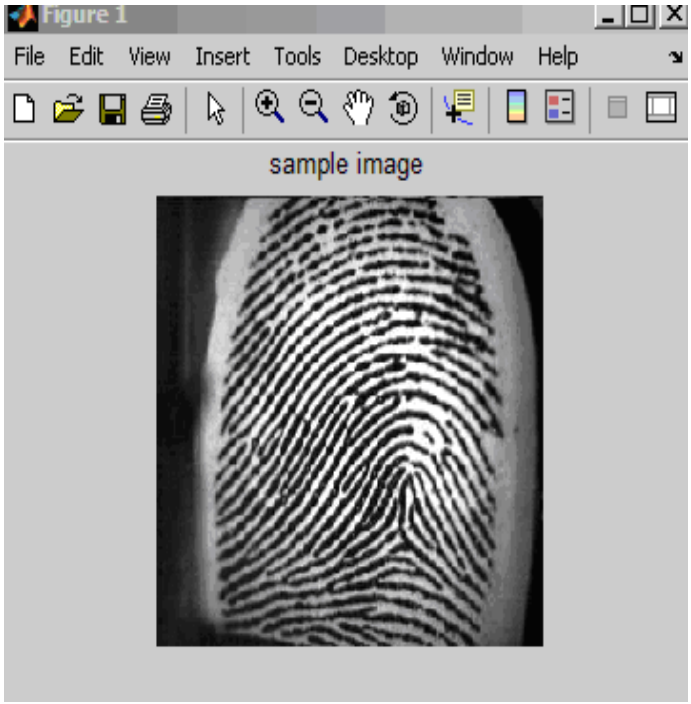

Fig 1. Sample Image

The 144 bit biometric key which is generated from the minutiae points is given below.

Columns 1 through 18

1 0 1 1 1 1 0 0 1 1 0 0 0 1 1 0 1 0

Columns 19 through 36

0 1 1 0 0 1 1 1 0 0 0 1 1 1 1 0 0 1

Columns 37 through 54

0 1 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 1

Columns 55 through 72

1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 1 1 1

Columns 73 through 90

1 0 1 0 1 1 1 0 0 0 0 0 0 1 0 1 0 0

Columns 91 through 108

0 1 1 1 1 1 1 0 1 0 1 1 1 0 0 0 0 0

Columns 109 through 126

0 1 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 0

Columns 127 through 144

1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 1 1 1

IV. BIOMETRIC KEY GENERATION FROM FACE

Biometric facial recognition systems measure and analyze the overall structure, shape and proportions of the face. Some features which are to be analyzed are distance between the eyes, nose, mouth, jaw edges, upper outlines of the eye sockets, size of the mouth, the location of the nose and eyes, the area surrounding the cheekbones. For the purpose of enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions. This can help to match with more accuracy. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded.

There are quite a few methods available for the generation of biometric key from facial feature. In this paper, a

method which consists of Radon transform and Fourier transform is used[6]. As some errors are bound to happen in the matching of faces, an error correcting algorithm is also to be used. Reed Solomon algorithm is used for this purpose.

A sample face is taken. The sample is subjected to radon transform, normalization, fourier transform, binarization and binary feature extraction. Then the error correcting reed-solomon code is used. The sample face image and the corresponding 14 bit biometric key obtained through the above mentioned process is given below.

1 1 1 0 1 1 1 0 1 0 1 0 0 1

V. TWO FACTOR BIOMETRIC KEY GENERATION

Generally, only one biometric feature is used to generate biometric key and based on this key encryption is done. As the biometric key is unique for a person, it is hard to break the encryption algorithm. A bogus biometric key may be used by intruder to deceive the system. To provide more security, one more biometric feature is added to generate another biometric key. The combination of two biometric keys can provide better security and this is known as 'Two Factor Biometric Key'.

As the generation of biometric key from face and finger print are discussed in the above sections, it is possible to have a biometric key from both these features. The biometric key which is generated from the fingerprint has 144 bits. Similarly the biometric key from the face has 14 bits. By combining these two keys in terms of bits, new biometric key can be generated. This new biometric key can be used for the encryption. As more than one biometric feature is required to break the encryption algorithm, it is highly impossible to do it though the intruders can possibly collect some data packets.

The combined key can be generated in many ways. One such algorithm is given here. The key generated from 'fingerprint' is of 144 bit length. Let this key is referred as 'K1'. Similarly, the key generated from 'face' is of 14 bit length. Let this key as 'K2'. The following algorithm is applied to these keys to get a two factor biometric key.

Step 1: The bits in the last two rows of 'K1'are removed. So the key is having 128 bits which is a standard key size for AES algorithm.

Step 2: The last six bits of 'K2' are to be removed. So, this key is having eight bits now.

Step 3: Each of the last bit in every column of 'K1' is to be removed.

Step 4: One bit of 'K2' in the order is replacing the removed bit in 'K1'.

Step 5: The modified 128 bit key is based on keys derived from both Finger Print and Face Biometrics.

The two factor biometric key generated as per the above algorithm is shown below.

Columns 1 through 16

1 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1

Columns 17 through 32

0 1 1 0 0 1 1 1 0 0 0 1 1 1 1 1

Columns 33 through 48

0 1 0 1 0 0 0 1 1 1 1 1 1 0 1 1

Columns 49 through 64

1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0

Columns 65 through 80

1 0 1 0 1 1 1 0 0 0 0 0 0 1 0 1

Columns 81 through 96

0 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1

Columns 96 through 112

0 1 0 1 0 0 0 1 1 1 1 1 1 0 1 1

Columns 113 through 128

1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0

The above generated two factor biometric key can be used as the key for any standard encryption algorithm such as AES.

Step 3 of the above mentioned algorithm can be modified such that the prediction is difficult for an intruder. Instead of the last bits in each row, one bit at random position may be removed and it can be replaced as per step 4.

The random position at which the bit of 'K1' is removed can be identified using pseudo-random generator. It can also be found out by the third 'zero' position from left or right.

It is also possible to use a combination of above mentioned algorithms or similar algorithms so that identification of position is to be made difficult to intruders if any.

VI. CONCLUSION

The proposed two factor biometric key authentication process for wireless networks is very dependable and highly reliable one. Though intruders outside can get some data packets due to availability of the radiated signal, it is highly impossible for them to break this biometric key as it involves two biometric keys and a unique algorithm.

Humans tend to leave lot of Finger Prints in outside world. That's why even the police use finger print identification. It is possible to get bogus finger prints easily. To over come this, this two factor biometric key can be used. Here an intruder has to get both the biometrics and their corresponding keys. Also he should know the algorithm with which the two factor biometric key authentication is done. This is highly difficult for any intruder. So, The wireless networks will be more secured if it employs two factor biometric key.

REFERENCES

[1] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, USA: CRC Press, pp 180, 1997.

[2] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Eugene Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human- Computer Studies, vol. 65, pp.744-757, 2007.

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," in Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.

[4] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[5] N.Lalithamani, K.P.Soman, "Irrevocable cryptographic key generation from cancellable finger print templates:An enhanced and effective scheme", European Journal of Scientific Research, pp 372-387, Vol. 31, No.3, 2009.

[6] B.Chen and V.Chandran,"Biometric based cryptographic key generation from faces", IEEE Conference on Digital Image Computing Techniques and Applications, 2007.

[7] Nalini Ratha, Jonathan Connell, Ruud M. Bolle, Sharat Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints", Proceedings of the 18th International Conference on Pattern Recognition, vol:4, Pages: 370 – 373,2006.