Network Security Using Biometric and Cryptography

Sandip Dutta, Avijit Kar, N.C. Mahanti, and B.N. Chatterji

Department of Computer Science and Engineering,
Birla Institute of Technology, Mesra, Ranchi - 835215, India
Tel.: +919431939630; Fax: +91-651-2275401
sandip_dutta2001@yahoo.co.in
http://www.bitmesra.ac.in

Abstract. We propose a biometrics-based(fingerprint)Encryption / Decryption Scheme, in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. From this unique key a random sequence is generated, which is used as an asymmetric key for both Encryption and Decryption. Above unique Key is send by the sender after Watermaking it in sender's fingerprint along with Encrypted Message. The computational requirement and network security features are addressed. Proposed system has a advantage that for public key, it has not to search from a database and security is maintained.

Keywords: DES, MD5, Biometric, Cryptography, Watermarking.

1 Introduction

Human life today revolves around a web of millions of computers networked together. While this network is very critical to make life beautiful, unscrupulous breaches can easily break the paradise we live in. It is, therefore, essential to be able to identify, verify the treats and safeguard the communication and computation network. True, the unscrupulous will soon catch up, but the challenge is to remain ahead. In this pursuit, inclusion of biometric data in communication is very successful today, basically for its enormity. Inclusion of biometric information like facial features, fingerprints, iris, retina, voice, signature strokes etc. in cryptography, further strengthens the communication security. Biometric is the biological characteristics, which is unique and measurable for automatically recognizing or verifying the identity of a human being. Biometric technologies for security includes recognition of faces, fingerprints, iris, retina, voice, signature strokes etc. Cr! yptography is an important security feature of computers. Information in computer can be secured by using many of the available cryptographic algorithms.

2 Previous Work

Very little work has been done generating keys using biometrics data because, with every sample, different templates are produced and cryptography relies on a

J. Blanc-Talon et al. (Eds.): ACIVS 2008, LNCS 5259, pp. 38–44, 2008.
© Springer-Verlag Berlin Heidelberg 2008

stable and unique key to encrypt and decrypt messages. For the incorporation of biometrics into cryptography there are two relevant approaches: key release and key generation. Key release algorithms described in the literature ([1],[2],[3],[4]) require that (1) the cryptographic key is stored as part of user's Database, (2) when matching with cryptographic key access to database is available, and (3) user authentication and key generation are two different processes. One problem with this algorithm is that there is no way to identify who produced the key and therefore, the user could deliberately choose a weak key. Besides, storing keys in a database is rather insecure as it could be easily hacked and lastly, an enrollment process is required to store the template. Key generation algorithms avoid some of the problems due to the key release algorithms by (1) binding the secret key to the biometric information and (2) not requiring to access the biometric template. Key generation literature is abound with the works of ([1],[4],[5],[6].[7],[8],[9],[10]) among others, in which key generation is more complicated than key release.

3 Finger Print with Cryptography for Network Security (Proposed Scheme)

Main features of the proposed method are the following

- For Sender
  - At first the recipient must provide his or her fingerprint at the sender's request.
  - Master fingerprint image is thus generated with the combination of the recipient's fingerprint image and the sender's fingerprint image.
  - A section(chance) from the master fingerprint image is taken to generate a key of 128 bits with the help of a standard hashing algorithm MD5.
  - The message which is intended to be sent to the receiver needs to be encrypted with standard DES algorithm. In the proposed algorithm from the 128 bit key a random sequence is generated depending on the length of the message and for every 64 bit message a separate 64 bit key is used to encrypt the message.
  - The sender's fingerprint is now watermarked by the random sequence generated from above mentioned step and the 128 bits key using wavelet transform based watermark method, in which first fingerprint image is decomposed into n level sub band images using DWT2 Haar transformation, producing LL, LH, HL, HH sub bands. Binary data is embedded into sub bands after multiplying with the gain factor. Watermarked image is obtained by IDWT2.
  - The fingerprint image thus watermarked along with the encrypted message is sent to the intended receiver.
- For Receiver
  - The recipient on receiving the watermarked image follows the Dewatermarking steps, using DWT2 and correlation vector, thereby extracting the random sequence and 128 bit key.

- The encrypted message will be decrypted with standard DES algorithm using asymmetric key, following the same steps as above of encryption i.e. every 64 bit message with separate 64 bit key using the same random sequence.

3.1 Description

Here in figure 1, we describe how the message is encrypted and decrypted. The recipient first provides his fingerprint as per request from the sender. The sender then merges the two fingerprints and only a portion of the merged image is taken to form the 128 bit master key with the help of MD5 hashing algorithm. A random sequence is generated depending on the length of the message. The message is then encrypted with the asymmetric key using DES algorithm. The master key along with the generated random sequence is watermarked in the sender's fingerprint. The watermarked image along with the encrypted message is sent to the recipient. Recipient first dewatermarks and gets the master key and the random

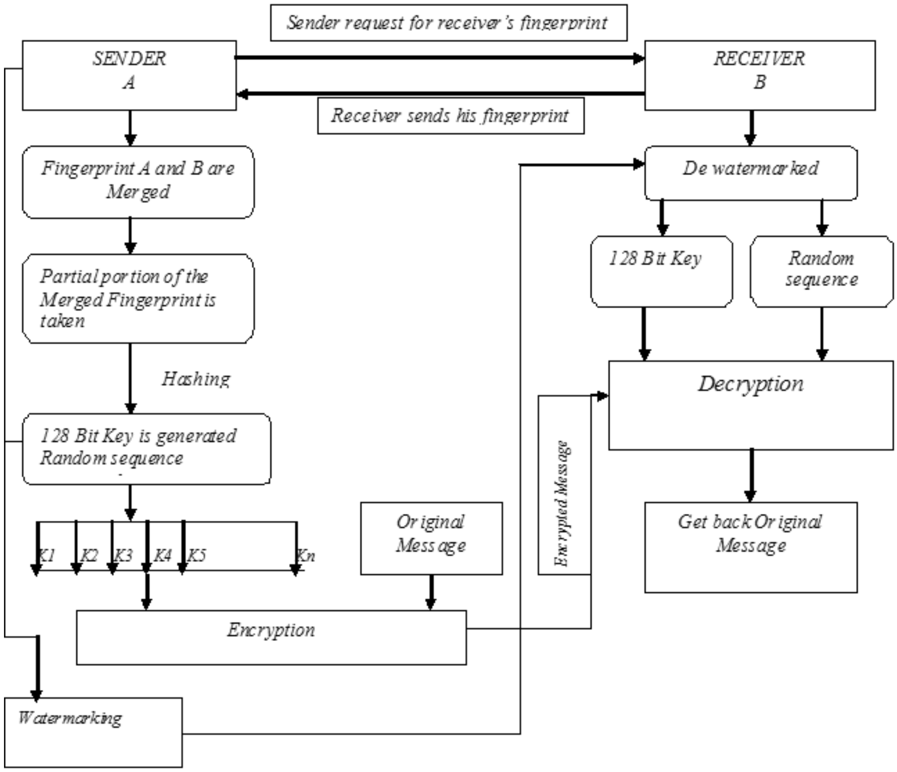
Sender request for receiver's fingerprint
SENDER A
RECEIVER B
Receiver sends his fingerprint
Fingerprint A and B are Merged
De watermarked
128 Bit Key
Random sequence
Partial portion of the Merged Fingerprint is taken
Hashing
Decryption
128 Bit Key is generated Random sequence
Encrypted Message
K1
K2
K3
K4
K5
Kn
Original Message
Get back Original Message
Encryption
Watermarking

Fig. 1. Proposed Encryption and Decryption methods

sequence. Encrypted message is now decrypted using the master key and the random sequence using DES algorithm.

1. Any rotation of the fingerprints would give rise to a separate 128 bit key, thus providing innumerable possibilities.
2. While taking a partial image from the master key, if the number of bits gets changed, a different key will be generated each time.
3. Using random sequence facilitates generation of a unique 64 bit key each time for the same message.
4. For each 64 bit information a separate 64 bit key is used for encryption.
5. Sender's fingerprint is watermarked with the random sequence providing the key with unique and robust characteristics, thereby making it impossible for an attacker/hacker to crack the key sequence.

4 Evaluation of Proposed Method References

Network security schemes are evaluated using several criteria as given in [11] and [12]. Evaluation of our scheme on these criteria are given below.

1. Uniqueness: The fingerprint image of sender and receiver combined to form unique characteristics. In the proposed algorithm, we are taking partial fingerprint, making intrusion very difficult.
2. Permanence: Till the fingerprint image is re-scanned the characteristics remain the same.
3. Universality: Fingerprints are universal characteristics.
4. Performance: The fingerprint identification accuracy should be achievable, with respect to the available resources and the identification should be achievable under all working conditions (e.g. environmental factors).
5. Collect Ability: The fingerprinting are evenly quantifiable.
6. Circumnavigation: It would be difficult to fool the system with fraudulent and inappropriate private keys.
7. Acceptability: The proposed biometric technique should be acceptable by the masses in this age of technology.
8. Storage Requirements: It basically refers to each party's quantitative information requirement to store subsequent information. Sender and receiver must not have to maintain a huge database.
9. Communication Requirement: Each party needs to provide his fingerprint to the other to generate the appropriate random key sequence.
10. Computational Requirement: Degree of computation needed by the persons involved in communication to generate the master fingerprints and random sequence with the fingerprints only. Computational time is negligible because no matching is involved with databases.
11. Implementation Costs: With vertical fall of the hardware cost the acquisition of finger scanner is very low.
12. Watermarking Scheme Support: Watermarking involving fingerprints are available using standard DWT2 and IDWT2 algorithms.

Table 1. Classes of Algorithms with Performan

Algorithm	Confidentiality	Authentication	Integrity	Key Management
Symmetric encryption algorithms	Yes	No	No	Yes
Public-key encryption algorithms	Yes	No	No	Yes
Digital signature algorithms	No	Yes	Yes	No
Key-agreement algorithms	Yes	Optional	No	Yes
One-way hash functions	No	No	Yes	No
Message authentication codes	No	Yes	Yes	No
Our algorithm	Yes	Yes	Yes	Yes

For the sake of completeness and comparison we are reproducing six algorithms the Table 10.1 in page 184 of the Schenier's book[13] and our algorithm in Tabel 1.

5 Analysis

We have timed, on message length, random sequence generation, encryption, watermarking, dewatermarking followed by decryption of the message, which is summerized in Table 2. Every time the program is executed a different random sequence is formed. For different lengths of bits taken from the merged fingerprint and rotation of any of the two fingerprints by two degrees clockwise, the master key changes as shown in the Table 3 and Table 4 respectively.

Table 2. No. of Characters vs. Time

No.of Characters in a message	Hashing (Sec.)	Encryption (Sec.)	WaterMarking (Sec.)	De Watermarking (Sec.)	Decryption (Sec.)
16	1.2168	0.24648	1.3542	0.9108	0.1560
32	1.2636	0.2496	1.3570	1.0140	0.2028
64	1.2168	0.3588	1.4570	1.0997	0.2808
112	1.2324	0.5928	1.5130	1.2320	0.4836

Table 3. No. of bits taken from master key vs. bits

No of bits taken from combined finger print	Hashing (Sec.)	No of bits changed (32bit in Hex)
10x10	0.0936	–
16x16	0.2184	31
24x24	0.5616	29
32x32	1.2324	31
42x42	2.9016	30

Table 4. No. of bits taken from master key vs. bits changed due to rotation

No of bits taken from combined finger print	Two degree clockwise rotation of receiver fingerprint, no of bits changed(32bit in hex)
10x10	30
16x16	32
24x24	30
32x32	30
42x42	31

6 Conclusion

The biometric key formed from the sender's and the receiver's fingerprints has many advantages over current authentication methods because it can neither be forgotten nor shared and is convenient for users to generate. The proposed method maintains security and integrity of the biometric data, which is so very important for network security. In the proposed scheme we are using DWT and IDWT for watermarking and dewatermarking, which is a nonlinear function, so exact sender's finger print could not be obtained. Work is on to address this problem.

References

1. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure smartcard-based fingerprint authentication. In: Proceedings ACM SIGMM 2003 Multimedia, Biometrics Methods and Workshop, pp. 45–52 (2003)
2. Soutar, C., Roberge, D., Stojanov, S.A., Gilroy, R., Vijaya Kumar, B.V.K.: Biometric encryption using image processing. In: Proceedings of the SPIE - Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pp. 178–188 (1998)
3. Roginsky, A.: A New Method for Generating RSA Keys. In: International Business Machines Consulting Group (2004)
4. Davida, G.I., Frankel, Y., Matt, B.J.: On enabling secure applications through offline biometric identification. In: Proceedings of the IEEE Privacy and Security, pp. 148–157 (1998)
5. Davida, G.I., Matt, B.J., Peralta, R.: On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Proceedings Workshop Coding and Cryptography, pp. 129–138 (1999)
6. Monrose, F., Reiter, M.K., Li, Q., Wetzel, S.: Cryptographic Key Generation from Voice. In: Proceedings IEEE Symposium on Security and Privacy (2001)
7. Monrose, F., Reiter, M.K., Wetzel, S.: Password hardening based on keystroke dynamics. In: Proceedings of the 6th ACM Conference of Computer and Communications Security, pp. 73–82 (1999)
8. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference of Computer and Communications Security (1999)

9. Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proceedings IEEE International Symposium on Information Theory (2002)
10. Linnartz, J., Linnartz, J.-P., Tuyls, D.: New shielding functions to enhance privacy and prevent misuse of biometric templates. In: Proceedings of the 4th International Conference on Audio and Video Based Person Authentication, pp. 393–402 (2003)
11. Costanzo, C.R.: Active Biometric Cryptography: Key Generation Using Feature and Parametric Aggregation. In: Second International Conference on Internet Monitoring and Protection, ICIMP 2007, July 1-5, p. 28 (2007)
12. Poh, G.S., Martin, K.M.: A Framework for Design and Analysis of Asymmetric Fingerprint Protocols. In: Third International Symposium on Information Assurance and Security, IAS 2007, August 29-31, pp. 457–461 (2007)
13. Schenier, B.: Applied Cryptography Protocol, Algorithms, and Source Code in C, 2nd edn., p. 184. Wiley Computer Publishing/John Wiley and Sons, Chichester (1996)
14. Choi, J.G., Sakurai, K., Park, J.H.: Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party. In: Zhou, J., Yung, M., Han, Y. (eds.) ACNS 2003. LNCS, vol. 2846, pp. 265–279. Springer, Heidelberg (2003)
15. Frattolillo, F., D'Onofrio, S.: A web oriented and interactive buyer-seller watermarking protocol. In: Security, Steganography, and Watermarking of Multimedia Content VIII, Proc. of SPIE-IS and T Electronic Imaging, vol. 6072, pp. 718–716 (2006)
16. Goi, B.M., Phan, R.C.W., Yang, Y., Bao, F., Deng, R.H., Siddiqi, M.U.: Cryptanalysis of two anonymous buyerseller watermarking protocols and an improvement for true anonymity. In: Jakobsson, M., Yung, M., Zhou, J. (eds.) ACNS 2004. LNCS, vol. 3089, pp. 369–382. Springer, Heidelberg (2004)
17. Ju, H.S., Kim, H.J., Lee, D.H., Lim, J.I.: An anonymous buyer-seller watermarking protocol with anonymity control. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 421–432. Springer, Heidelberg (2003)