ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

Cryptographic Technique Using Biometric Authentication

Sanjukta Pal[1], Prof (Dr) Pranam Paul[2]

Research Scholar, Department of Computer Application, NIT Durgapur, West Bengal, India

Professor, Department of Computer Application, Narula Institute of Technology, Agarpara, West Bengal, India

ABSTRACT: In recent days, for secure information transaction through internet, the most used term is cryptography. Where encryption algorithm, decryption algorithm, key generation algorithm and key matching algorithms are used for proper secure transaction from sender to receiver, avoiding any middle attacker. Here the main concept of the paper comes from cryptography, which is combined with the fingerprint geometry, which is the current leader of Biometric Authentication. Here the fingerprint geometry is used for key generation, information deduction from the key. Here the fingerprint matching algorithm would be used for information deduction from key. To implement the above concept, sender's recent fingerprint geometry would be used to construct key by combining it with the information. For key decryption, the sender's Database fingerprint images, which are already kept by receiver at receiver's end would be used. Here the fingerprint matching algorithms would be used, which are applied on the binary conversion of the fingerprint images. For this purpose the whole technique is applicable on the binary form. So, for another part of cryptography, means for encryption and decryption process, the binary form of the data is taken. So the steps may be applicable on any type of data, means text, image, multimedia, graphics data etc.

KEYWORDS: Cryptography, encryption, decryption, key, recent fingerprint geometry, database fingerprint geometry.

I. INTRODUCTION

For secure information transaction through internet, Cryptography is used. Here for secure data communication the plain text would be encrypted into cipher text using encryption process. This encrypted text along with the key or information would be send by the sender at receiver's end. Then using the key or information, the receiver would decrypt the encrypted text. Using this base idea there exist different algorithm for encryption and decryption and for key generation. This paper is on same concept of cryptography, where plain text would be encrypted using encryption algorithm. After that, the encrypted text along with information would be achieved. Next, the information would be combined with the sender's fingerprint image, which would be called as key. After reaching the encrypted text along with key at receiver's end, the receiver would try to collect information from key using the Database fingerprint images of sender (which are already given to the receiver by sender).With the help of fingerprint matching algorithm or key matching algorithm, the receiver would try to match the sender's fingerprint geometry with the key. If the two matches (i.e. if one of the Database fingerprint image matches with the key's fingerprint geometry) then the information can be derived from key. Otherwise the information cannot be derived. At next step, after getting the information, the receiver would decrypt the encrypted text using that information.

Here the whole cryptographic process is done on the binary conversion (i.e. the encryption process would be done on the binary form of the plain text, so the reverse technique means decryption process also done on binary form. Also, for the key construction, the information and the fingerprint geometry is also taken in binary format. Finally, the fingerprint geometry matching or key matching algorithm is also applicable only on binary format of fingerprint geometry). For the application of binary conversion as a whole, this cryptographic technique is applicable on any type of data transmission.That means, it is applicable on the text, image, multimedia data etc. which can be converted into binary form.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

In this cryptographic technique, for generation the key, the sender's recent fingerprint geometry would be combined with the information.On the other hand, for deriving the information from key, the sender's Database fingerprint geometry would be used. Here sender's database fingerprint geometry is nothing but the collection of sender's fingerprint images already kept at receiver's side. For information deduction from the key, any one fingerprint geometry matching algorithm would be used [19] or [20] or [21].

II. RELATED WORK

The basic advantages of using biometric authentication with cryptography are, any type of failure handling, false reading handling speed limit accuracy and forgeries. For these reason there exists so many research work on biometric authentication in combination with cryptographic technique. In [21], the biometric approach combined with cryptographic technique is provided, for high security over traditional cryptography avoiding any type of risks and middle attacks. Here biometric technologies like fingerprint geometry, eye scanning (iris and retina scanning), hand geometry, face recognition, voice recognition, signature, key stroke are used. Again esoteric biometrics like facial thermographs, DNA matching, palm vein pattern are also be applicable. Here biometric is used, because biometric cannot be stolen, lost or forgotten and be always available. Here, proper framework has not been used. In [22], fingerprint encryption technique is discussed for ATM banking system. Here, for authentication purpose users would use smart card as well as fingerprint geometry. In first layer, for authentication smart card would be used and in the second layer authentication process, the biometric fingerprint technique would be used.

In [23], a provably secure and blind authentication protocol has been proposed based on asymmetric encryption of biometric data. These protocol is applicable on multiple biometrics because of no restrictive assumptions. This protocol is not affect able on the accuracy whenever encryption key acts as an additional layer security. Here, locking and unlocking method is used for performing authentication to provide strong encryption, non-repudiable authentication, and protection against replay, client side attack and recoverability. In [24], biometric characteristics has been used as cryptographic key to secure transfer. Here biometric hashes are used for authentication. In this type of biometric cryptography, biometric characteristic would be extracted and processed into biometric hashing, which would help the decryption process by finding the key pair. Here, the key pair may be of public key or private key and the technique is applicable in large domain.

III. PROPOSED WORK

The idea of combining biometric authentication with cryptography is not only for better security but also for implementation and technical simplicity. Because this cryptography with biometric authentication is capable to handle any type of failure handling, enhance speed limit and false reading handling. So, here total cryptographic technique (Encryption process as well as decryption process) has been developed with the help of fingerprint geometry, the current leader of biometric authentication. Here the total technique is discussed in some individual steps, at first at sender's side and then at receiver's side. Starting from sender's side encryption process to receiver's side decryption process some steps are followed. Those are defined distinctly step wise and chronologically, first at sender's side and then at receiver's side.

A. STEPS AT SENDER'S SIDE

At sender's end, the binary format of the normal text would be taken as plain text. So,

Step 1: the plain text would be encrypted by encryption process, from which we will get the encrypted text and some Information.
Step 2: the information would be combined with the sender's recent fingerprint geometry for key generation.
Step 3: encrypted text along with key would be send by the sender.
Step 4: finally the information would be send by the sender to the receiver side.

The steps at Sender's side is diagrammed in figure 1. Here, at first at sender side the binary form of plain text would be encrypted by encryption process. After that the sender would get the two parts, one is the encrypted text and another is the information. Next, the information would be combined with the binary form of sender's recent fingerprint geometry

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

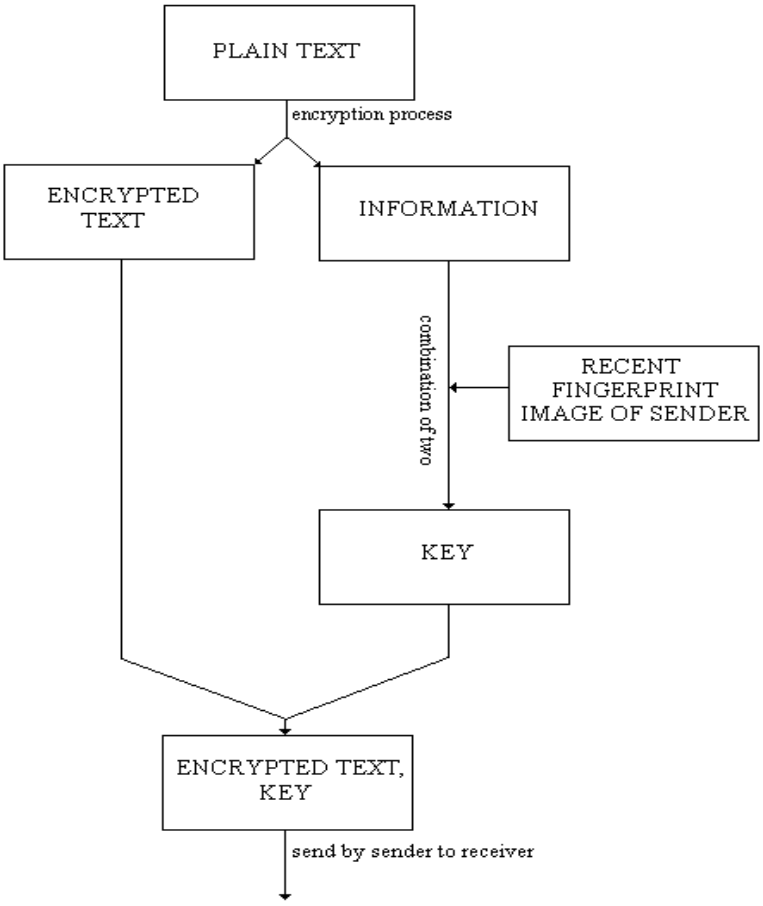
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

and the key would be formed. Finally the key along with encrypted text would be send by the sender at the receiver's end.

Fig.1: AT SENDER'S SIDE



B. STEPS AT RECEIVER'S SIDE

At receiver's end,
Step 1: encrypted text along with key would be accepted by the receiver
Step 2: the encrypted text and the key will be separated.
Step 3: with the help of sender's database fingerprint geometry(which are kept by the receiver) and the fingerprint Geometry matching algorithm the information would be deducted from key. If, the two images does not match, information cannot be received.
Step 4: with the help of information the encrypted text would be decrypt into plain text or in the original binary form of the plain text or normal text.

The steps at Receiver's side is diagrammed in figure 2. Here, at first the receiver would get the encrypted text along with key. The using database fingerprint geometry of the sender kept by the receiver and with fingerprint matching algorithm the information would be deducted from the key. Finally the information would help to convert the encrypted text into decrypted text or plain text. Here also the whole process would be held on the binary conversion.

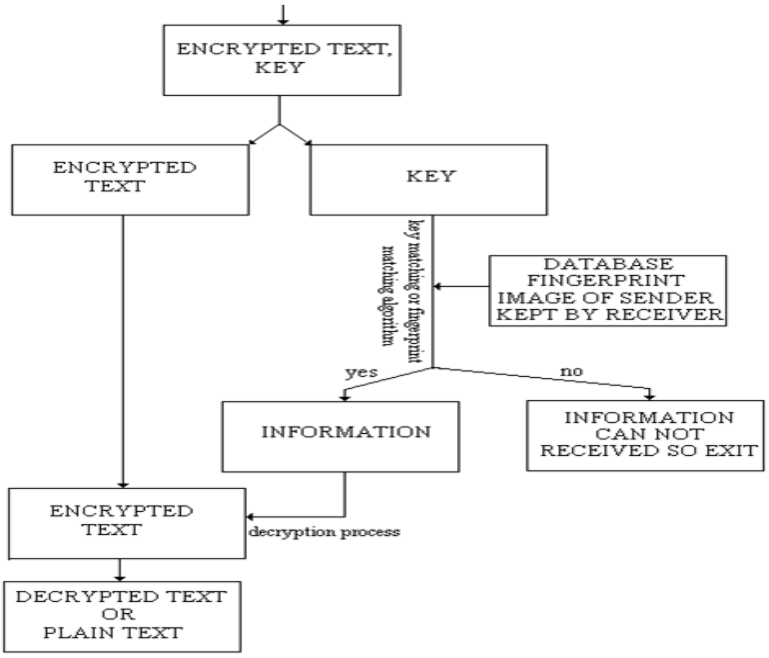
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

Fig.2: AT RECEIVER'S SIDE



IV. PERFORMANCE APPRAISAL

In the whole scenario, the sender's fingerprint geometry (one is recent fingerprint geometry and the another are Database fingerprint geometries) is used for both encryption and decryption. No other fingerprint images can derive the information from key, which can help the decryption process. So it can be concluded, that the technique is symmetric key cryptography and also called as private key cryptography.

For its symmetric key nature, the total cryptographic technique is fast and efficient. But the classical symmetric key cryptography suffer from big disadvantage, because the use of same key and key exchange without letting anyone. This cryptographic technique would avoid that disadvantage, because here the key is formed by using fingerprint geometry combined with information (in classical cryptography only information is used as key). On the other hand, for key exchange, the information cannot be derived if the two fingerprints (one is recent fingerprint image and another is database fingerprint image) does not match. So, it can be concluded that being a symmetric key cryptography, it is advantageous like asymmetric key cryptography and secure enough.

V. CONCLUSION

In this cryptographic technique the biometric authentication concept is here incorporated with information for key formation. Here it can easily said that this cryptographic technique is a symmetric key cryptography because only one person's (here sender's) fingerprint geometry is used for key formation, so this technique is fast and efficient and also same advantageous like classical asymmetric key cryptography. This cryptographic technique would avoid the disadvantage of classical symmetric key cryptographic, because here the key is formed by using fingerprint geometry combined with information (in classical cryptography only information is used as key). On the other hand, during key exchange, the information cannot be derived if the two fingerprints (one recent another database fingerprint image) does not match, which concludes better security. The only disadvantage is the probability of stolen the sender's database fingerprint geometry. Our future work is to work on better security by maintaining the simplicity and to reduce the time complexity for whole technique using the base idea of cryptographic technique using biometric authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

REFERENCES

1. J. K. Mandal, S. Dutta, "A 256-bit recursive pair parity encoder for encryption", Advances D - Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE, France), www. AMSE-Modeling.org,Vol. 9 nº1-2, pp. 1-14, 2004.
2. Pranam Paul, Saurabh Dutta, "A Private-Key Storage-Efficient Ciphering Protocol for Information Communication Technology", National Seminar on Research Issues in Technical Education (RITE), National Institute of Technical Teachers' Training and Research, Kolkata, India,March 08-09, 2006.
3. Pranam Paul, Saurabh Dutta, "An Enhancement of Information Security Using Substitution of Bits Through Prime Detection in Blocks", Proceedings of National Conference on Recent Trends in Information Systems, (ReTIS-06), Organized by IEEE Gold Affinity Group, IEEE Calcutta Section, Computer Science & Engineering Department, CMATER & SRUVM Project-Jadavpur University and Computer Jagat, July 14-15, 2006.
4. Dutta S. and Mandal J. K., "A Space-Efficient Universal Encoder for Secured Transmission", International Conference on Modelling and Simulation,MS' 2000 – Egypt, Cairo, pp 11-14,April 2000.
5. Dutta S., Mal S., "A Multiplexing Triangular Encryption Technique – A move towards enhancing security in ECommerce", Proceedings of IT Conference (organized by Computer Association of Nepal), BICC, Kathmandu 26 and 27 January, 2002.
6. Paul Reid, Biometrics for Network Security, Prentice Hall PTR, chapter-5, 2003.
7. A white paper by the University of Southern California and VeriSign,"Building a Security Framework for Delivery of Next Generation Network Services", United States, 2005.
8. L. Podio and Jeffrey S. Dunn "Biometric Authentication Technology: From the Movies to Your Desktop", National Institute of Standards and Technology (NIST), Information Technology Laboratory 497, 2002.
9. Edited by Lori Ayre, Infopeople Project, Library Computer and Network Security Infopeople Project, http://infopeople.org/howto/security/, 2003.
10. Sarbari Gupta, "Identity Authentication Identity Authentication using the using the PIV Token PIV Token", National Institute of Standards and Technology, India, 2004.
11. "Authenticating with one of the safest devices: the biometric Sony Puppy, Secure Computing Corporation", 4810 Harwood Road, San Jose, CA 95124 USA, 2001.
12. Biometric Consortium web site: http://www.biometrics.org 2006.
13. International Biometric Industry Association, http://www.ibia.org 2005.
14. Bioenable Technologies Pvt. Ltd. http://www.bioenabletech.com/ biometrics_india_pune_contact.htm, 2004-2005.
15. "Fingerprint Identification system", Securitex Electronic Systems Engineering, http://www.securitex.com.sg/, 2006.
16. "Finger print sensors technology overview", Manvish Embedded Services, http://www.manvish.com/embedded/miFAUN/techoverview.php, 2006.
17. "Biometric Fingerprint Security", TopAZ Solutions Pte Ltd, http://www.topazsol.com/bio_door_access.htm, 2006.
18. Sanjukta Pal, Dr. PranamPaul , "Cryptographic protocol Depending on Biometric Authentication", accepted and published in International Journal of Engineering Science and Technology (IJEST), ISSN No. 0975-5462, Vol. 5 No.02, pp. 354-358, February 2013.
19. Sanjukta Pal, Sucharita Pal, Dr. Pranam Paul "Fingerprint Geometry matching by Divide and Conquer Strategy" accepted and published in International Journal of Advanced research in Computer Science(IJARCS), ISSN No. 0976-5697, Volume 4, No. 4, March-April 2013**.**
20. Sanjukta Pal, Sucharita Pal, Dr. Pranam Paul "Matching of Fingerprint Geometry by Advanced Divide and Conquer Technique" accepted and published in International Journal of Advanced research in Computer Science(IJARCS), ISSN No. 0976-5697, Volume 4, No. 4, March-April 2013**.**
21. Abanti Cyrus Makori, "Integration of Biometrics with Cryptographic Techniques for Secure Authentication of Networked Data Access", Integration of Biometrics, http://cit.mak.ac.ug/iccir/downloads/ICCIR_09/Abanti%20Cyrus%20Makori_09.pdf,
22. Fengling Han, Jiankun Hu, Xinhuo Yu, Yong Feng, and Jie Zhou, "A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications", Springer-Verlag Berlin Heidelberg, ICB 2006, LNCS 3832, pp. 675 – 681, 2005.
23. K Hemanth, SrinivasuluAsadi, DabbuMurali, N Karimulla andM Aswin, "High Secure Crypto Biometric Authentication Protocol", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , pp- 2496-2502, 2011.
24. TonimirKisasondi, Miroslav Baca, AlenLovrencic, "BIOMETRIC CRYPTOGRAPHY AND NETWORK AUTHENTICATION", Journal of information and organizational sciences, Volume 31, Number 1, pp- 91- 99, 2007.

BIOGRAPHY

Sanjukta Pal is research Scholar at NIT Durgapur, she has completed M.Tech (CST) and MCA under the West Bengal University of Technology and B.Sc in Mathematics from The University of Burdwan. She has total 3 International. Her research interests are internet security and cloud computing.

Dr Pranam Paul is a Professor of Narula Institute Technology, Agarpara He had completed his Ph.D from Electronic and Communication Engineering department of National Institute of Technology, Durgapur in the field of Cryptography and Network Security. His research interest is internet security. His research interest is internet security.