Digital Signature using Biometrics

Deep Mann, Shashank Gupta, Ankit Sharma, Shakil Akhtar

***Abstract*—It is desirable to generate a digital signature using biometrics but not practicable because of its inaccurate measuring and complex methodologies, without using specific hardware devices that hold signature keys or biometric templates securely. Proposed model resolves the problem in biometric based digital signature by making it simple and secure. Proposed model uses the biometric template and generate the key which uses the AES which is much secure to make the signature useful.**

***Index Terms*— Authentication, digital signature, biometrics, symmetric key, hash.**

I. Introduction

Biometric technologies that are capable of identifying individuals through one-to-many matching across large shared databases can provide convenient authentication services for many applications, including information security, physical access, financial services, etc. without requiring costly and time-consuming re-enrollment for each application. But the potential for shared access and multiple uses of biometric databases raises serious concerns with respect to personal privacy because biometric templates are considered by some to constitute personal information that could be used for unauthorized purposes. The standardization of template formats, intended to promote deployment by enabling sharing of costly enrollments, has in addition created security vulnerability. An enrollment or recognition template created for one purpose could be misappropriated and used for fraudulent purposes. And unlike a PIN or password, a biometric template cannot be changed, recovered, or reissued if it is compromised [1]. By their nature, biometric entities are stable over time; otherwise their utility would be quite limited. A digital signature is a term used to describe a data string which associates a digital message with an assigned person only. It has various applications in information security such as authentication, data integrity, and non-repudiation. One inevitable drawback of the cryptographic schemes is that the signer must carefully hold and possess a signing key which is not memorable at all. It is desirable occasionally to derive the signing key from a human source, say biometrics, rather than keeping it in an external hardware device. Biometrics is actually the science of using digital technologies to identify a human being based on the individual's unique measurable biological (say physiological or behavioral) characteristic such as fingerprint, voice pattern, iris pattern, face, retina, handwriting, thermal image, or hand print.

It is widely recognized that (automatic) identification is the most suitable application for biometrics [14, 16]. In some sense, the digital signature can be compared to a biometric signature that is verified by capturing a real hand-written signature. However, it is technically hard to apply biometrics directly to the digital signature because of its inaccurate measuring and potential hill-climbing attacks [22].Recently several studies have been done in the subject of using biometrics for generating a digital signature.

One potential means of protecting stored templates is encryption, but because the matching algorithms used to match templates and thereby authenticate an individual identity cannot, in general, operate on such encrypted templates, the templates must be decrypted prior to matching. Thus the decrypted templates are inevitably exposed to potential hacker attacks when matching is being performed. The management and protection of private keys also presents challenges that are well-documented. Furthermore, cryptographic algorithms can be computationally expensive and limit the capacity of large-scale biometric systems to provide responsive authentication services. So the use of the biometric as a key is a good concept because it cannot be stolen easily but the major concern is how to generate key from a template so we proposed a solution to generate key from biometric template and use it in creating digital signature.

II. Proposed Method

1) Biometric Template Transformations

We describe here a means for transforming a biometric template so that it assumes a new format that is unique to a particular application. Such a transformed template cannot be successfully matched to a second template extracted from the same biologic entity unless the second template is transformed so that its format is identical to that of the first template. Thus a template generated in a format corresponding to a particular application A could not be misappropriated and used to authenticate a user for application B because the enrollment database for application B would have a different format than those enrolled for application A. Consider biometric templates T_1 and T_2 derived from the same biologic entity (hand, finger, eye, etc.) such that an appropriate matching function M (T_1, T_2) has a value:

$$\mathbf{M\ (T_1, T_2) = 1} \qquad (1)$$

if the templates are judged to match (i.e. to have come from the same biologic entity) and

$$\mathbf{M\ (T_1, T_2) = 0} \qquad (2)$$

Deep Mann is Asst. Prof., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:er.deepmann@gmail.com

Shashank Guta is M.Tech., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:coolshashank22@rediffmail.com

Ankit Sharma is M.Tech., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:erankitsharma1991@gmail.com

Shakil Akhtar is Engineer IV Software Engineer, Cisco, Bangalore, India; e-mail:Shakilsoz17ster@gmail.com

ISBN: 978-988-19253-6-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

If the templates are judged to not match. Assume first that templates T_1 and T_2 are generated in exactly the same way with the same format so that if they do indeed come from the same biologic entity, M (T_1, T_2) will have a value of 1.

Now we apply a transformation F_A to the "root" templates T_1 and T_2 so that the transformed templates $F_A(T_1)$ and $F_A(T_2)$ have a unique format specific to a particular use or application A. We desire that the transformation F_A have the property that the matching process is invariant under the transformation, that is,

$$\mathbf{M(F_A(T_1), F_A(T_2)) = M(T_1, T_2)} \qquad (3)$$

This invariance is important because it means that matching can be performed on the transformed templates, making it unnecessary to reverse the transformation, recreating and exposing the root templates T_1, T_2 prior to or during the matching process.

2) Overall Design of Model

The overall design of the model is shown on fig 1. Our model uses the matched template and use the templates as a key in the encryption of message digest to create the digital signature.

Our model can be explained in following steps:

A. Match the template to authenticate user.
B. Save the template as a string.
C. Create a hash of string created by template.
D. Create message digest by creating hash of message.
E. Encrypt the message digest by created hash of template.
F. The encrypted digest is the required signature, attach it with the message and send to receiver.

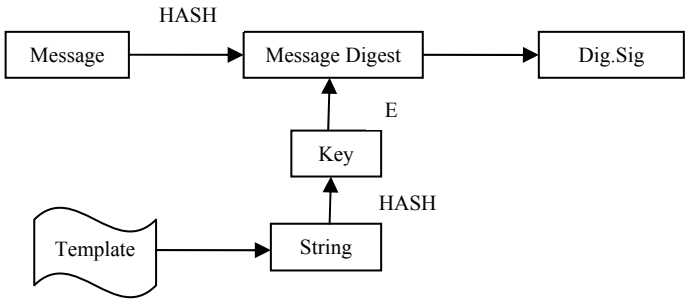

Fig 1. Overall Design of Proposed Model

III. Conclusion

Proposed model resolves the various problem of creating digital signature with biometric template. It is strong and esy to implement so can be used at almost every place with any biometric template. Its future work is to make sure the correct encryption technique to make it fast and secure. As proposed model gives the solution to create secure keys from biometric template so it resolves many problems in cryptographic and security world.

References

[1] M. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Transactions on Information Theory, vol.36, no.3, May 1990.

[2] M. Bellare and R. Sandhu, "The security of practical two-party RSA signature schemes," Manuscript, 2001.

[3] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," Notices of the American Mathematical Society (AMS), vol. 46, no. 2, pp.203-213, 1999.

[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N0.292," Eurocrypt '99, Lecture Notes in Computer Science vol. 1592, Springer- Verlag, pp.1-11, 1999, and IEEE Trans. on Information Theory, vol. 46, no. 4, 2000.

[5] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," Asiacrypt'01, Lecture Notes in Computer Science vol. 2139, Springer-Verlag, pp.514-532, 2001.

[6] C. Boyd, "Digital multisignatures," Cryptography and Coding, Oxford University Press, pp.241-246, 1989.

[7] S. Brands, Rethinking public key infrastructures and digital certificates, The MIT Press, p.11 and pp.219-224, 2000.

[8] H. E. Burke, "Handbook of bar Coding Systems," Van Nostrand Reinhold, New York, N.Y., 1984.

[9] Daon Inc., "Biometric Authentication & Digital Signatures for the Pharmaceutical Industry," White paper available at http://www.daon.com/downloads/publications/esignature.pdf

[10] J. Daugman, "High confidence personal identifications by rapid video analysis of iris texture," IEEE International Carnahan Conference on Security Technologies,pp.50-60, 1992.

[11] J. Daugman, "High confidence personal identifications by a test of statistical independence," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.15, no.11, pp.648-656, November 1993.

[12] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through offline biometric identification," IEEE Symposium on Security and Privacy, pp.148-159, 1998.

[13] Denso Inc., "QRmaker: User's Manual," Denso Corporation, Aichi, Japan, 1998.10 T. Kwon and J. Lee

[14] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM Journal of Computing, vol.17,no.2, pp.281-308, Apr. 1988.

[15] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, February 2000.

[16] P. Janbandhu and M. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, vol.9, no.5, pp.205-212, 2001.

[17] V. Maty´aˇs and Z. ˇR´iha, "Biometric authentication - security and usability", Manuscrypt available at http://www.fi.muni.cz/usr/matyas/cms matyasriha biometrics.pdf

[18] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, pp.287-291, pp.312-315, 1997.

[19] R. Nagpal and S. Nagpal, "Biometric based digital signature scheme", Internet- Draft, draft-nagpal-biometric-digital-signature-00.txt, May 2002.

[20] Roger. C. Palmer, "The Bar Code Book," Helmers Publishing, Peterborough, N.H., 3rd Ed., 1995.

[21] P. Orvos, "Towards biometric digital signatures," Networkshop, Eszterhazy College, Eger, pp.26-28. March 2002.

[22] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol.21, pp.120-126, 1978.

[23] C. Soutar, "Biometric system performance and security," Manuscrypt available at http://www.bioscrypt.com/assets/bio paper.pdf, 2002.

[24] C. Soutar, D. Roberge, A. Stoianov, R. Golroy, and B. Vijaya Kumar, "Biometric Encryption," ICSA Guide to Cryptography, McGraw-Hill, 1999, also available at http://www.bioscrypt.com/assets/Biometric Encryption.pdf

ISBN: 978-988-19253-6-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)