I. J. Computer Network and Information Security, **2017, 1, 12-19**
Published Online January 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.01.02

A Novel Digital Signature Algorithm based on Biometric Hash

Shivangi Saxena Research Scholar
Uttar Pradesh Technical University, Lucknow, India
E-mail: saxena.sh28@gmail.com

Darpan Anand Assistant Professor
Hindustan Institute of Technology and Management, Agra Uttar Pradesh Technical University, Lucknow, India
E-mail: darpan.anand.agra@gmail.com

Abstract—Digital Signature protects the document`s integrity and binds the authenticity of the user who have signed. Present Digital Signature algorithm confirms authenticity but it does not ensure secrecy of the data. Techniques like encryption and decryption are needed to be used for this purpose. Biometric security has been a useful way for authentication and security as it provides a unique identity of the user. In this paper we have discussed the user authentication process and development of digital signatures. Authentication was based on hash functions which uses biometric features. Hash codes are being used to maintain the integrity of the document which is digitally signed. For security purpose, Encryption and Decryption techniques are used to develop a bio -cryptosystem. User information when gets concatenated with feature vector of biometric data, which actually justifies the sense of authentication. Various online or offline transaction where authenticity and integrity is the top most priority can make use of this development.

Index Terms—Hash functions, Bio-cryptosystem, Feature vector, Digital Signature, Integrity, Authenticity, Biometric Template.

I. Introduction

Authentication is the proof that the message was sent by the original sender from it where it was generated. To affirm the authenticity and non-repudiation Digital signatures has been used to ensure the original source of the message. For authentication and security purposes, various biometric traits like fingerprint, palm print, iris etc. are being used because of their unique characteristics and consistent behavior over time. Being a unique characteristic trait, biometrics have been treated as the most secure way for authentication, but it has some vulnerabilities and weak points identified by *Ratha et al.* in 2001 [8]. For the purpose of providing secrecy, encryption is being implemented with biometric traits which is termed as biometric cryptosystem.

In the Biometric cryptosystem [1] security of data and its authentication uses the public key cryptographic algorithm which can be called as digital signatures algorithm.

The biometric template matching also has various strategies for its comparison [2].The helper data [3] is being used for generating keys and stores biometric features for further matching. For the purpose of secured transaction of data its security has been accomplished with digital signature.

The digital signature is the way of data security and maintaining its integrity in which string of zeros and ones are generated by the algorithm [4] for authentication. Digital signatures have been used in almost every electronic field for the purpose of security of the stored template data. It is a public key cryptographic algorithm which is designed in concern of authenticity of a digital message/document. A private key is used to sign a message to be transmitted and the public key correspondingly verifies the signature. Thus, the any party can verify the signed message/document by a private key. A valid digital signature is a sign to believe that the message was sent by a known user and its integrity is not hampered in transit. Digital signatures have been used in many fields of electronic transactions and data security like e-commerce, banking applications, information security etc.

In electronic transaction data authentication and its integrity must be verified, the digital signature makes sure that the data has not been modified or altered after subscribed by the sender`s side. Hashing is the crucial part in the formation of digital signatures.

Dutta et al, proposed the technique of creating digital signature. Hashed file has been made and then creation of signature has been done which includes a pair of keys to encrypt and decrypt the message. A variable size hashed file was obtained with their algorithm.

In digital signatures the whole message is not used, in place hash function is applied to the arbitrary size of message which gives a fixed size of message digest. There various hashing techniques and best hashing strategy has been chosen for the given data pattern and there are various forms of hashing like Dynamic hashing, Cryptographic hashing, Input Data Hash, Geometric hashing, Robust hashing, Bloom hash, String hashing but which one to choose is a different process[5]. Whereas

the hashing methods are different way, it includes ways of adding the additional hash values to the key which must be uniformly distributed over the whole range of its index. If the security of the private key has been compromised then it would be a critical situation to guess the validity of the digital signature. Hashing itself is a numeric based so, hashing tables are not suitable for some problems like unordered, multidimensional, prefix searching for long and variable length keys, data which is not unique, and dynamic data.

Most preferably string hashing operation is done which enquires hash table.

Clam Vielhauer et al [7], calculated the biometric hash vector for each feature vector. Feature vector of a biometric characteristic have different points to be counted while working on them, like in iris only alignment is necessary while with fingerprints it is not sufficient, and we need other features too.

In our paper, we are applying hash functions on the extracted feature vectors of the user`s finger print and storing it as template data after encryption which forms bio-cryptosystem. The idea of storing the data in encrypted form was derived from [6] where feature vectors and password are stored together in a template. It checks the integrity by again calculating hash value on biometric template to enhance the security of the biometric templates and to ensure the user is legitimate or not in electronic transaction. Hash functions are being imposed and hash values of the template data are calculated to obtain a digital signature. Biometric combining with the hash value gives more security and authentication as it becomes more vulnerable against attacks in online services. Then we have also develop digital signatures based on biometric hash. It is a signature obtained from the combination of the input message or document on which hash functions has been applied. Fig. 1 describes the introductory phase of the algorithm.

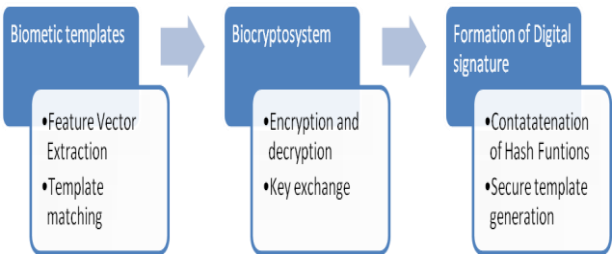

Fig.1. Process of Introduction

Any biometric characteristics could be chosen for applying hash functions but here we are working with finger prints. The algorithm SHA-256 is being applied for creating hash functions.

It provides a more secure way to store and transit biometric templates as used in e-passport [20] and e-transactions. Digital signature obtained from the hashed biometric traits is authentic way of obtaining a digitally signed document. Algorithm works in various phase like registration phase, which includes key exchange with Diffie-Hellman key exchange with other relevant features of the user, another is login phase, it includes feature vector and other user information works as user ID. Further the decryption process will reveal its authentic identity. User will first register to the system and then login with the user`s finger print, if it finds that the user is authentic the user is allowed to access the system with his or her account. The user can sign a document digitally with this biometric hash based technique.

Paper is being organized in various sections, after introduction, second section describes the related and previous work studied. Third section is the propose work and the algorithm developed. The fourth section is the analysis of the proposed algorithm with respect to security and the last section is all about concluding the work and what else could to be done in future time for the enhancement of the algorithm. At last is the reference, which is the list of all referred articles in the research.

II. Related Works

For biometric securities and verification it is necessary to have proper technique for biometric matching. There are various techniques of feature extraction for different biometric traits and template matching using a combination of ISEF edge detection and contour based biometric recognition algorithm [17]. Various morphological approaches have been developed for image feature extraction [18]. Here we have obtained minutia as a feature vector by *Vahid. K. Alilou* et al influenced by the work of *Joshua Abraham* et al [19]. It is technically very difficult to apply directly biometric traits to the digital signature because it may result inaccurate value and attacks like potential hill-climbing attacks [9]. Various studies have been done in the field using biometrics for generating a digital signature [10]. Encryption is one of the potential means of template's protection, but authentication cannot be done with these encrypted templates. Thus, templates need to be decrypted and exposed to several attacks prior to matching. The basics of creating Digital Signature by biometrics have been described by obtaining secure keys [10]. Traditionally, digital signatures, smart cards were used to sign because they have the cryptographic keys stored in them [11]. The documents need to sign in such a way that true identity must be cross verified to avoid various attacks reported in [12] [13]. That's the reason of choosing biometric characteristics. Biometric key based digital signature has been developed in which biometric key has been applied on the hash value of the document [14]. *Taekyoung Kwon et al,* proposed the first practical method for biometric based digital signature where RSA can be applied without losing its security [15].

Clam Vielhauer et al, proposed the approach to generate hash values based on statistical features in online signature signals [7]. It is a secure and stable hash which is not possible by any forgery to reproduce another hash vector [7].Our work has been efficiently influenced by the work of *Ahmed B. Elmadani et al,* [16].

Our work is primarily based on the authentication of biometric system. The various online transaction needs to be more secure while using biometric traits. As, biometric system securities are also hindered by various attacks. By imposing hash techniques a secure digital signature can be obtained. Digital signatures are usually be used for authenticity of the user side. When we talk about Biometric traits it gives a unique hash code for the unique user which states that the message is sent by the authentic user and hence a valid signature is generated. High confidentiality of messages security is more important for sender authentication, especially in financial context like online transaction and authentication. Digital signatures are being increasingly used in e- transactions and for email services. The two most common secure e-mail systems using digital signatures are Pretty Good Privacy and Secure/Multipurpose Internet Mail Extension [3]. Secure Electronic Transaction (SET) is most spread use of credit card transaction over the internet. So, it is a patent need to secure the data, for which we have proposed bio-cryptosystem with hash functions which protects the data from being maliciously altered, it ensures authentication, non-repudiation and validation of the electronic document.

III. The Proposed Work

The proposed work is basically for the authentication of the user and security of the data using biometric traits, we are here working with finger prints. Bio-cryptosystem is developed by encrypting the feature vector file of the user by Elgamal Encryption which uses a private key obtained by Diffie-Hellman algorithm and for enhancing its authenticity SHA-256 hash function has been used to obtain unique code. General Biometric working lacks in security and authentication sometimes that's the reason for generating Digital Signature by imposing hash function. Feature vector extracted from biometrics works data file for further processing. Here we have saved the minutia points of the biometric data as the extracted feature vector in a text file working as a template. The idea of template saving was drawn from [20]. The algorithm works in two phases, first is registration phase and another is login phase.

Registration Phase: It is a two way communication between sender and receiver. Fig.2 illustrates it.

Algorithm1: Initialization and Registration Phase.

1. Start
2. At Sender side.
3. $K_{session}$ key is obtained from Diffie-Hellman algorithm.
4. Sender gives finger print and ID.
5. FV is the extracted features of the finger print.
6. EM=Elgamal Encryption using $K_{session}$ (ID | | FV | |*h*(ID | | FV))
7. EM is send to Receiver.
8. At Receiver side
9. Decrypt EM with $K_{session.}$
10. If Matched
11. Success message send to Sender.
12. End

(i) (i) Sender is the one who wishes to get enrolled in the system. The Sender gets registered by providing its fingerprints and user ID to the system.

(ii) A key named as the $K_{session}$ is exchanged between sender and receiver by Diffie-Hellman algorithm and Feature vector i.e. minutia points are extracted and saved in a text file as a template for further matching and verification.

(iii) Receiver obtains the extracted feature and the private key of the user which is developed using Diffie-Hellman algorithm and further encrypts it using Elgamal Encryption.

(iv) At the receiver end it decrypts using $K_{session}$ key, if the decrypted data is same as the encrypted one, then a success message of user registration is sent to sender.

Login Phase: It uses the Encryption Key obtained from the registration phase.

Algorithm 2: Login and verification phase.

1. Start
2. At User/Sender side
3. Request for login.
4. Input the login details (Finger Print and UID).
5. FV extracted from finger print.
6. Calculate Integrity check IC=h (FV| |ID).
7. Calculate Authentication Data,
   AD= (FV| |ID| |IC).
8. At Receiver side
9. Matches the FV of user and stored at the time of registration, if matched
10. Calculate integrity check with stored FV,
    i.e. ICs=h(FVs| |ID).
11. If IC=ICs
12. Success login.
13. Else exit.

(i) User access the system to login with his user ID and fingerprint and obtains a feature vector file which is saved as a template for further authentication.

(ii) Now, the system calculates Integrity check i.e. the hash of user ID and feature vector, it is further used to calculate Authentic Data to verify the user and make a successful login.

(iii) The generate hash code was done by SHA- 256 technique.
(iv) The receiver checks the user authenticity with by matching the feature vector file of the claimed user with the one stored in the database with the same ID. If both are the same files, it checks the hash values of the concatenated user feature vector and ID to the stored feature vector and ID, if both the integrity checks are same file.
(v) The User will have the success login.

It gives a unique hash code for every authentic user .So, it's a triplet authentication process as it is secured by unique biometric trait, user information and unique hash code.

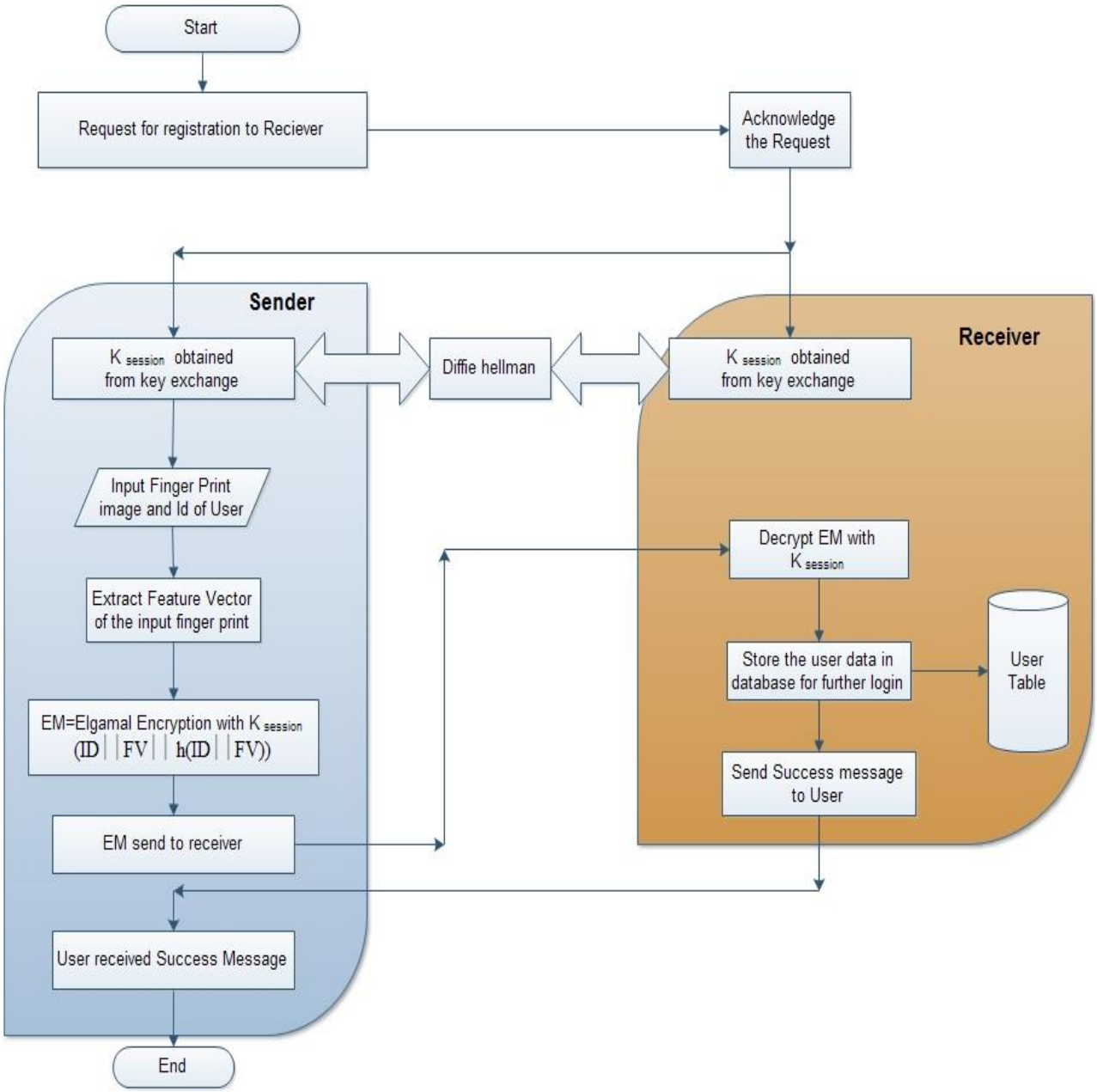

Fig.2. Registration Phase

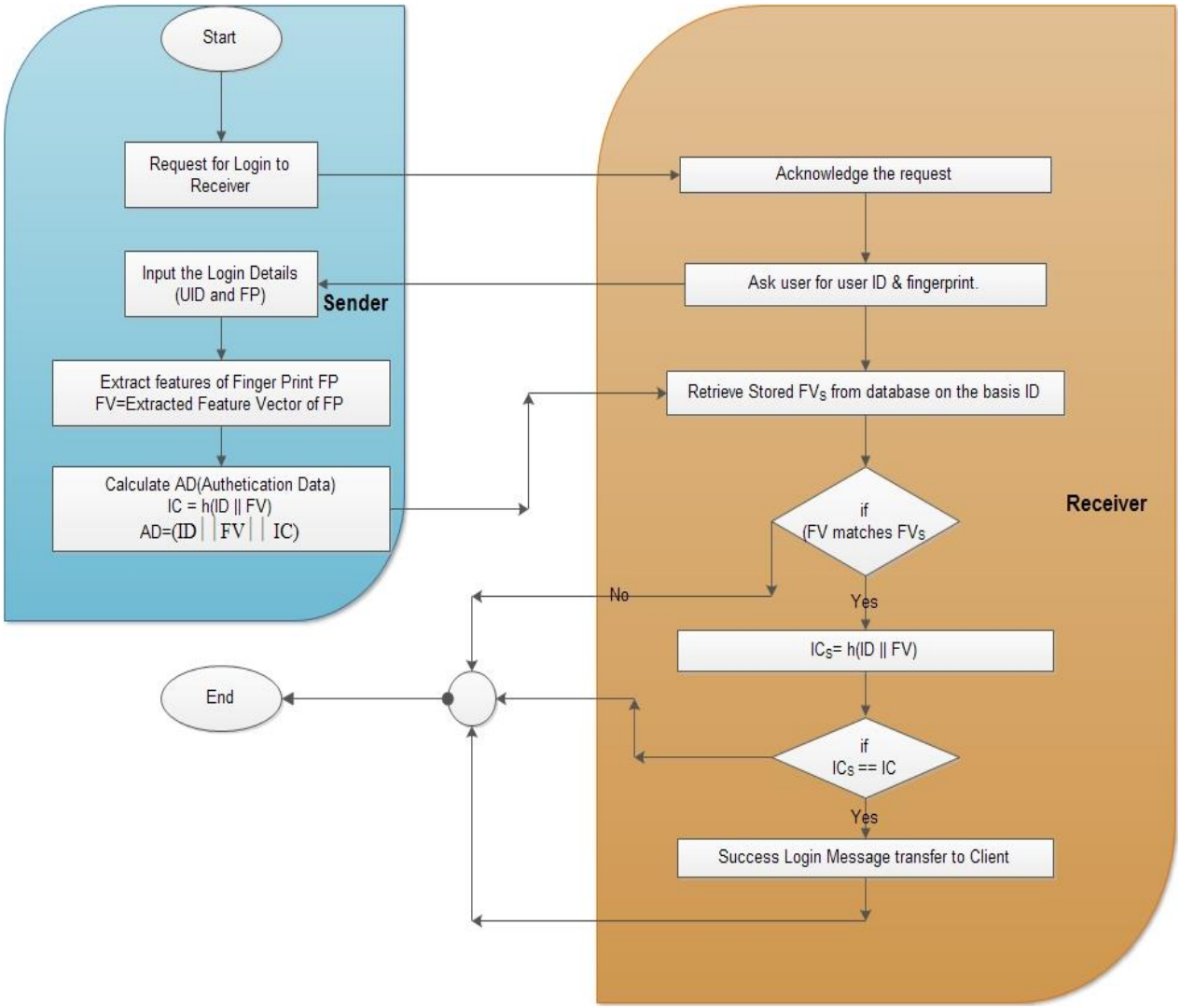

Fig.3. Login Phase

Digital Signature Generation: For protecting the document and its controlling its authenticity and integrity.

Algorithm3: Signature Generation

1. Start
2 .User ID, Finger Print & a nuance
3. Calculate H=*h* (Doc| |FV| |nuance)
4. ED=Elgamal Encryption (H)| |Doc| |FV (Digitally Signed Document)
5. ED send for verification.
6. End

(i) To make a document digitally signed user gives the ID, fingerprint and a nuance chosen by him.
(ii) A unique hash code is generated by concatenating the document, feature vector and the nuance.
(iii) The generated hash code is encrypted and send with document and user `s feature vector.
(iv) It is finally verified whether an authentic user has digitally signed the document or not.

Algorithm4: Signature Verification

1.Start
2.Decrypt ED ➔ H'| |Doc| |FV.
3.if H'=H
4.Check if FV'=FV
5.Signature successfully verified
6.else
7.Signature verification failed.

(i) To verify the authenticity of the digital signature it checks by decrypting the hash value both matches it further checks feature vector of the user have signed the document with stored feature vector.
(ii) If both matches then signatures are valid otherwise not. Thus, digital signature obtained here are much secure than ordinary one because we have

calculated the hash values of the biometric feature which were concatenated with some other user information which gives a ultimate way to sign a document digitally.

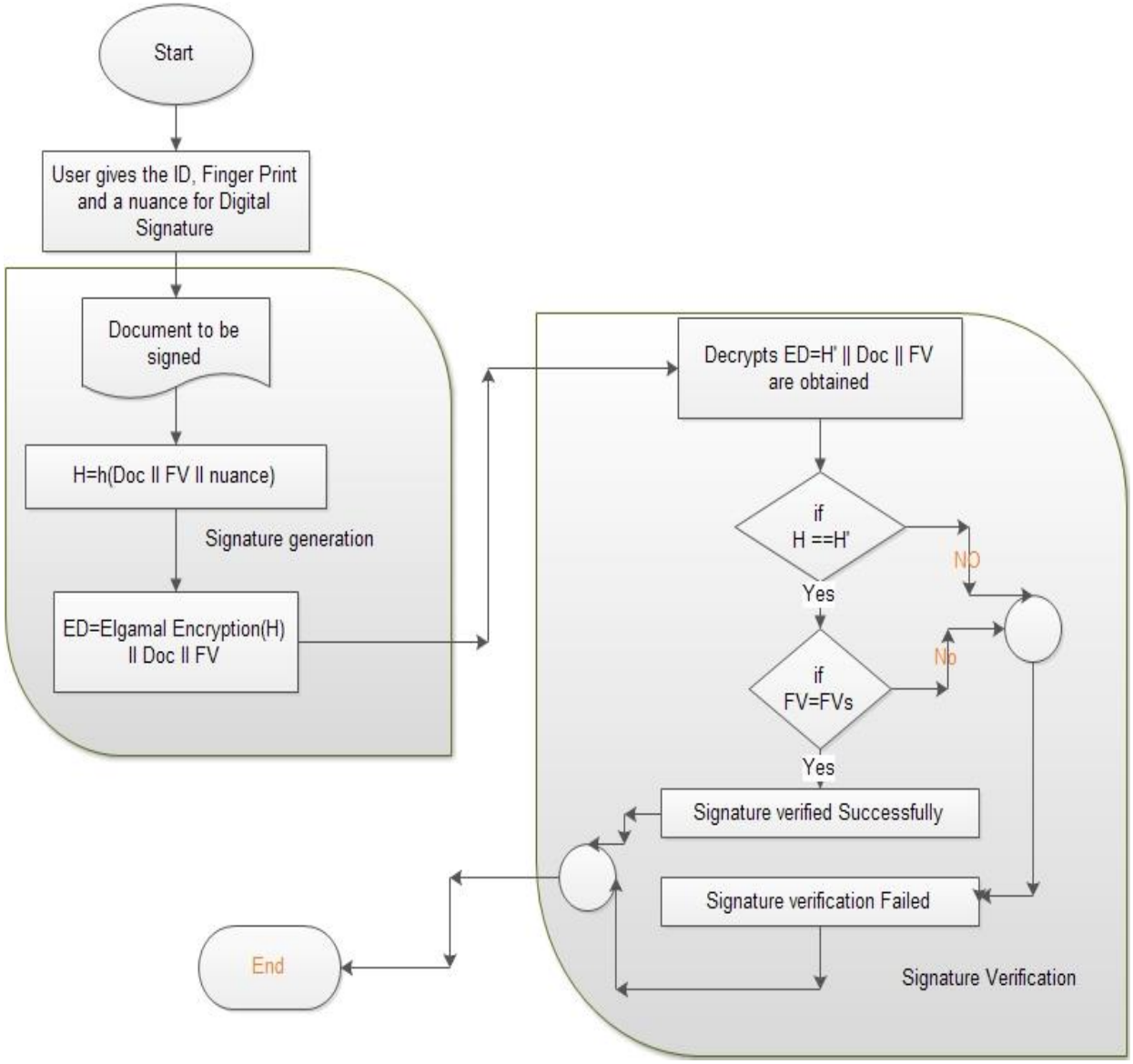

Fig.4. Digital Signature Generation

IV. Security Analysis

Our Proposed algorithm serves the purpose to secure the integrity of the data as it robust to various kinds of attacks like:

Chosen Plaintext Attack – In this the attack has the pair of cipher text-plaintext. He just needs to determine the encryption key. In our algorithm security is given by two more layers, user biometric and unique hash code generation, so even if the key is determined by the attacker it is impossible to determine the user biometric features. So, the attacker fails to attack our algorithm.

Known Plaintext Attack − In this attacker is aware of the plaintext for some volume of the cipher text. Attacker, only needs to decrypt the rest of the cipher text. But, in our algorithm cipher text is also protected by hash of biometric traits, so it is almost impossible to reach the original plain text.

Dictionary Attack – In this attack, attackers build a dictionary of cipher text and its corresponding plain text, but our system generates a unique code every time which is generated by the user`s biometric. So, there is no chance of getting hit by the attacker.

Cipher text Only Attacks (COA) − In this attack, the attacker can access to the cipher text(s) but he can`t access the corresponding plaintext. In our algorithm attacker can`t access the cipher text as it undergoes in hash generation which a unique entity every time. So, even if cipher is known the attack can`t access our algorithm.

Man in Middle Attack (MIM) − The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

But in our algorithm other than the encryption with public key there are other perspectives of security like biometrics and hash values concatenation. So, our algorithm can`t be hit by this attack.

Birthday Attack − This attack is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates. Let us assume the first student's birth date is 3rd Aug. Then to find the next student whose birth date is 3rd Aug, we need to inquire $1.25*\sqrt{365} \approx 25$ students.

Similarly, if the hash function produces 64 bit hash value, the possible hash values are 1.8x1019. By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about 5.1x109 random inputs. If the attacker is able to find two different inputs that give the same hash value, it is a collision and that hash function is said to be broken, but our algorithm also gets concatenates with other features which reduces the chances of being broken.

Brute Force Attack (BFA) − In this method, the attacker tries all possible combinations to determine the key. Our algorithm has multiple layers of combination of uniqueness as it is also secured by biometric hash over the simple Elgamal encryption, which is a unique value for every user. So, there is not a single possible combination to get the key by the attacker.

Side Channel Attack (SCA) − This type of attack is developed to exploit the weakness of physical implementation of the system. Hence our cryptosystem is enough developed to overcome the weakness, it provides a high sense of security and authentication.

V. Conclusion

The Proposed work is a secure way of authentication as encryption is also based on large primes and a unique hash template is generated. It provides a more secure way to user authentication in e-transactions and other online applications. Our proposed algorithm proves a secure way of authentication as compared to other biometric based securities because our work concatenates encryption with hash function which gives a unique way to check the integrity, whereas other proposed algorithm relies only on encrypted only [21]. Fingerprints are being used as the biometric trait in our work, it can also be done with other biometric features like palm veins, iris, retina etc. There may be other ways of unique template generation for a secure authentication. In future time this work may be implemented on web to resolve the issue of authentication and loss of integrity.

References

[1] U. Uludag, S. Pankanti, A.K. Jain, "Biometric cryptosystems: Issues and Challenges", IEEE Multimedia.

[2] Emanuele Maiorana, Patrizio Campisi, Alessandro Neri “TEMPLATE PROTECTION FOR DYNAMIC TIME WARPING BASED BIOMETRIC SIGNATURE AUTHENTICATION”, 5-7 July 2009 IEEE.

[3] Digital signatures S.R. SUBRAMANYA AND BYUNG K. YI.

[4] Security for Digital Rights Managmement, Vol. 92, No.6, pp: 948960, 2004 Jain AK, Nandakumar K, Nagar A: Biometric template security. EURASIP J Adv Signal Process 2008, 1-17.

[5] Choosing Best Hashing Strategies and Hash Functions Mahima Singh,. Deepak Garg Computer science and Engineering Department, Thapar University, Patiala.

[6] Password Hardened Biometric: A Complete Solution of Online Security, I. J. Computer Network and Information Security, 2013, 6, 42-48 Published Online May 2013 in MECS.

[7] Biometric Hash based on Statistical Features of Online Signatures Clam Vielhauer', Ralf Steinrnetz', Astrid Mayerhofer'.

[8] Ratha, J. Connell, and R. Bolle. 2001. Enhancing Security and Privacy in Biometrics-based Authentication Systems. IBM Systems Journal 40, 3 (2001), 614–634.

[9] 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.

[10] Digital Signature using Biometrics D Mann, S Gupta, A Sharma, S Akhtar - Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I WCECS 2015, October 21-23, 2015, San Francisco, USA.

[11] Elmadani A. B, Prakash V and Ramli A. R.Application of Smartcard & Secure Coprocessor, BICET conference. Brunei.2001.

[12] Spalka A. Cremers A and Langweg H.,Protecting the Creation of Digital Signature with Trusted Computing Platform Technology Against Attacks by Trojan Horse. In IFIP Security Conference. 2001.

[13] Langweg H. Malware Attacks on Electronic Signatures Revisited. In Sicherheit 3rd Jahrestagug Fachbereich Sicherheit der Gesellschaft fuer Informatik. 2006.

[14] Trusted Document Signing based on use of biometric(Face) keys International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 289-296 The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012) Ahmed B. Elmadani.

[15] Practical Digital Signature Generation using Biometrics, Taekyoung Kwon1 and Jae-il Lee2.

[16] Digital Signature forming and keys protection based onperson’s Characteristics Ahmed B. Elmadani Dept. of Computer Science Faculty of Science Sebha University, 978-1-4673-1166-3/12/$31.00 ©2012 IEEE.

[17] International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014 ISSN 2091-2730182 www.ijergs.org Biometric Template Feature Extraction and Matching Using ISEF Edge Detection and Contouring Based Algorithm Deven Trivedi1, Rohit Thanki1, Ashish Kothari2 1PhD Researcher Scholar, C. U. Shah University, Near Kothariya Village, Wadhwan City, Gujarat, India 2Assistant Professor, Atmiya Institute of Technology & Science, Rajkot, Gujarat, India.

[18] Image Feature Extraction for application of Biometric Identification of Iris – A Morphological Approach JOAQUIM DEMIRA JR.1, JOCELIMAYER2 Proceedings ofthe XVI Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI’03) 1530-1834/03, 2003 IEEE.

[19] Joshua Abraham, "Fingerprint Matching using A Hybrid Shape and Orientation Descriptor", State of the art in Biometrics, ISBN 978-953-307-489-4, July 2011.
[20] Evolution of Electronic Passport Scheme using Cryptographic Protocol along with Biometrics Authentication System, I. J. Computer Network and Information Security, 2012, 2, 50-58 Published Online March 2012 in MECS.
[21] Mohammad Ziaullah; Dept. of ECE, SECAB I.E.T, Vijayapur, Karnataka, India; Prakash Shetty; Shoaib Kamal, "Image feature based authentication and digital signature for wireless data transmission".IEEE, 7-9 Jan. 2016.

Authors' Profiles

Shivangi Saxena, born in 1991. M.Tech candidate in Uttar Pradesh Technical University, Lucknow, India. Her main interest lies in Cryptography and Network security.

Darpan Anand is working as Assistant Professor in the Department of Computer Science and Dean (Student Welfare) at Hindustan Institute Technology & Management, Agra. His research interest includes Network Security, Cryptography, Computer Network and Distributed Computing.

How to cite this paper: Shivangi Saxena, Darpan Anand,"A Novel Digital Signature Algorithm based on Biometric Hash", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.1, pp.12-19, 2017.DOI: 10.5815/ijcnis.2017.01.02

