Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering — CSEE 2013

ISBN: 978-981-07-5461-7

Validation of RNA-FINNT for Reduction in Error Percentage

Kuljeet Kaur, Dr.G.Geetha

Abstract*— Fingerprint is used as an Identity Authentication Parameter. RNA-FINNT is a Fingerprint Hash Algorithm which is used to extract the hash code value of fingerprint when it is used for identity authentication. This algorithm is already validated on two parameters: reduction in number of angles and removal of dependency on global features. But this paper elucidates the third parameter which is error percentage that how RNA-FINNT has resulted in reduction in error percentage. Detailed analysis of existing algorithms (Grid Hash, Angle Hash and Minimum Distance Hash) is done on the basis of number of minutiae points extracted and on the behalf of which corresponding error percentage is calculated. Proof is generated through mathematical calculation that increase in the number of minutiae points in RNA-FINNT would result in decrease of error percentage. Validation is done that execution of RNA-FINNT results in reduction of error percentage.

Keywords*— Network Security, Reduction in Error Percentage, Minutiae Points, Algorithm, Fingerprint Hash, Error Percentage.

I. Introduction

Identity Authentication is required for verification of the legitimate user. There are various authentication parameters which could be used for verification process like Voice Recognition, Iris, Location- Based, Smart Card, Password and Fingerprint etc. On the basis of a Survey done by us it is analyzed that Fingerprint is the most acceptable identity authentication parameter in future and higher is the evaluation of security and privacy in online transactions if fingerprint is used as an authentication type [1]. So fingerprint is used as an identity authentication parameter for security purposes in the public network. Fingerprint is of three types: Arches, Loops and Whorls, its brief description is as follows [2]:

i. Arches (It may be plain (ridge enters from one side, make a wave in the center and flow in the opposite side) or tented (angle is there in arch). Delta is not there in arch.
ii. Loops (ridge count is there). One core and delta is there in loop.
iii. Whorls (Any fingerprint that has two or more delta's is whorl). In it one ridge would be having 2 delta's.

There exist three technologies which could be used to extract the value from the fingerprint. Following are the technologies for finger print authentication [3]:

i. Correlation (where image itself is used as a template): It is very easy to recreate fingerprint from templates, and which would give access to unauthorized users so it is not safe to use.
ii. Texture Descriptors (fingerprint texture is used): captures global and local features of a fingerprint in a compact fixed length vector which would be finger code.
iii. Minutiae Descriptors (set of unique features in finger print): Everyone falls into one of the above said categories. Within these three categories there are thirty different minutiae points. This makes fingerprint unique because no one has the same number of minutiae points on the same place.

Correlation and Texture Descriptors give access to unauthorized users so we have not used these technologies for extracting the value of fingerprint. Minutiae Descriptors is used as a technology and new algorithm RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm) is derived for extracting the value of fingerprint [3]. Drawbacks of existing algorithms (Grid Hash, Angle Hash and Minimum Distance Hash Algorithm) were considered in developing this new algorithm (RNA-FINNT) [3].

It is proved that RNA-FINNT has resulted in the following benefits [3]:

1. Reduced Number of Angles
2. Removal of Dependency on Global Features
3. Rapid Execution as takes less time in Calculation.

This paper focuses on the new benefit which is proof of reduction in error percentage with the use of RNA-FINNT. The structure of the remainder of the paper is as follows. In Section II proof is generated for reduction in error percentage with the implementation of RNA-FINNT for the extraction of fingerprint value. In Section III elucidation is upon possibility of complete network security with the use of RNA-FINNT and Section IV concludes the paper.

Kuljeet Kaur
Lovely Professional University Punjab (India)

Dr.G.Geetha
Lovely Professional University Punjab (India)

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering — CSEE 2013

ISBN: 978-981-07-5461-7

II. Proof of Reduction in Error Percentage with the Implementation of RNA-FINNT for the Extraction of Fingerprint value

Whenever a fingerprint is to be matched in the forensic labs hardly minimum of 8 to 12 minutiae points are considered [4]. If only 8 minutiae points get matched then fingerprint is considered to be matched. So existing algorithms focuses on only extracting 8 to 12 minutiae points. But RNA-FINNT helps in extracting more than 15 minutiae points. We have already discussed that total number of minutiae points on a fingerprint is 30 so if only 8 minutiae points would be considered for fingerprint matching then 30% is the error percentage [5] [6]. But if 12 minutiae points would be considered some mathematical calculation is required to justify that error percentage would be reduced from 30% for existing algorithms also.

$$Reduction\ in\ Error\ for\ Existing\ Algorithms = r_1(e)\ ,$$

$$Reduction\ in\ Error\ for\ RNA-FINNT\ Algorithm = r_2(e),$$

$$Error\ Percentage = e(p)\ ,$$

$$Overall\ Reduction\ in\ Error(When\ tm(p)\ are\ increased) = \Delta r(e)$$

$$Number\ of\ Minutiae\ Points = m(p),$$

$$Increase\ in\ Number\ of\ Minutiae\ Points = \Delta m(p)\ ,$$

$$Total\ Number\ of\ Minutiae\ Points\ for\ Consideration = tm(p)\ ,$$

$$New\ Calculated\ Error\ Percentage = e_1(p)\ ,$$

Proof*: *For Existing Algorithm

$$m(p) = 8\ , e(p) = 30\ , \Delta m(p) = 4\ ,$$

$$tm(p) = m(p) + \Delta m(p) = 8 + 4 = 12,$$

$$e_1(p) = \frac{(e(p) * m(p))}{tm(p)} = \frac{30 * 8}{12} = 20 \quad \textbf{(1)}$$

$$i.e\ New\ Calculated\ Error\ Percentage\ is\ 20.$$

$$r_1(e) = e(p) - e_1(p) = 30 - 20 = 10 \quad \textbf{(2)}$$

8 minutiae points are considered error percentage is 30%. But if 12 minutiae points are considered then according to (1) error percentage would be 20%. So overall reduction in error percentage if number of minutiae points are 12 according to (2) is 10.In our algorithm RNA-FINNT number of minutiae points considered is more than 12 so the error percentage reduces as the number of minutiae points into consideration is increased. If 15 minutiae points are considered then following is the proof for reduction in error percentage.

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering — CSEE 2013

ISBN: 978-981-07-5461-7

$$\boldsymbol{Proof: For\ RNA-FINNT}$$

$$m(p) = 8\,, e(p) = 30\,, \Delta m(p) = 7\,,$$

$$tm(p) = m(p) + \Delta m(p) = 8 + 7 = 15,$$

$$e_1(p) = \frac{e(p) * m(p)}{tm(p)} = \frac{30 * 8}{15} = 16 \quad \textbf{(3)}$$

$$i.e\ New\ Calculated\ Error\ Percentage\ is\ 16.$$

$$r_2(e) = e(p) - e_1(p) = 30 - 16 = 14 \quad \textbf{(4)}$$

$$\Delta r(e) = r_2(e) - r_1(e) = 14 - 10 = 4$$

$$\boldsymbol{i.e\ Overall\ Reduction\ in\ Error\ when\ tm(p) is\ increased\ is\ 4}$$

If 15 minutiae points are considered then according to (3) error percentage would be 16. So, overall reduction in error percentage in RNA-FINNT according to (4) is 14. So when number of minutiae points would be increased then overall error percentage would be reduced. Mentioned below is the overall error reduction if 15 minutiae points are considered (as per RNA-FINNT) instead of 12 (as per Existing Algorithms) is:

$$\Delta r(e) = r_2(e) - r_1(e) = 14 - 10 = 4$$

$$i.e\ Overall\ Reduction\ in\ Error\ when\ tm(p) is\ increased\ is\ 4.$$

As per Equation (4) reduction in error percentage is 14 when the number of minutiae points considered is 12 and as per Equation (2) reduction in error percentage is 10 when the number of minutiae points considered is 15. So, overall reduction in error percentage would be calculated by subtracting equation (2) from equation (4).

So proof is generated with this example that as the number of minutiae points increase in RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm), the error percentage while identifying the legitimate user would reduce.

III. POSSIBILITY OF COMPLETE NETWORK SECURITY WITH THE USE OF RNA-FINNT

As fingerprint is the most acceptable identity authentication parameter so it should be used during the process of communication at the transport layer. Whenever a Session is created between the Client and the Server security of the data becomes prime concern. Generally organizations use password based key exchange authentication but fingerprint should also be used along with Password for enhancing the security at the transport layer. Assimilation of Password and Fingerprint should be done for generating an Ideal Password Authentication Scheme [7]. We have derived a framework in which RNA-FINNT is used to extract the values of fingerprint and enhancement of the security at the transport layer is done [7]. This framework would enhance the security as the security checks are performed at Client and Server side both. Following is the sequence of security checks which overall fortifies the transport layer:

- First security check is with Username. (Client side security is verified either the client is legitimate or malicious)
- Image (Server reverts back with image which was initially stored by the User while inserting data through Login Form of the Framework [7]. Client has to validate that the image reverted back is matching and would be matched with the hash code value already stored in the database then Server side security check would be done)
- Middle Finger (Server has to get verification of the Client. Value of the middle finger would be extracted already stored in the database through Login Form of Framework [7].If it gets matched the client side second security check would be done)

ISBN: 978-981-07-5461-7

- Password (Third Client side security check would be done with Password. If it gets matched with the stored value at the Database then client side complete security check is done [7])
- Index Finger (When Client side security check is done the complete security check for Server is required. It is done with the index finger fingerprint of the user. If it gets matched with the stored value in the Database then Server side security check is complete [7])

This framework would be implemented on the Data Center specifically on the Transport Layer and overall enhancement of this layer would be done.

Case Study: Lovely Professional University has its own Data Center which is capable of handling 30K users at the same span of time. Clustering is done and the network is divided into Zones. All Application Servers are connected with the Database Server and Reporting Server *(Figure 1)*. Storage Area Network is connected with the Database Server *(Figure 1)*. Whenever any report is required by any application server same would be provided by the Reporting Server *(Figure 1)*. This framework would be implemented on the Application Servers and complete Multi Server Environment would be generated. Complete security would be provided at the Client and Server side both with the successful implementation of this framework.

From Figure 1 it is clear that clustering is done and complete Database is prepared on all the Application Servers. Reports required could be derived from the Reporting Servers.

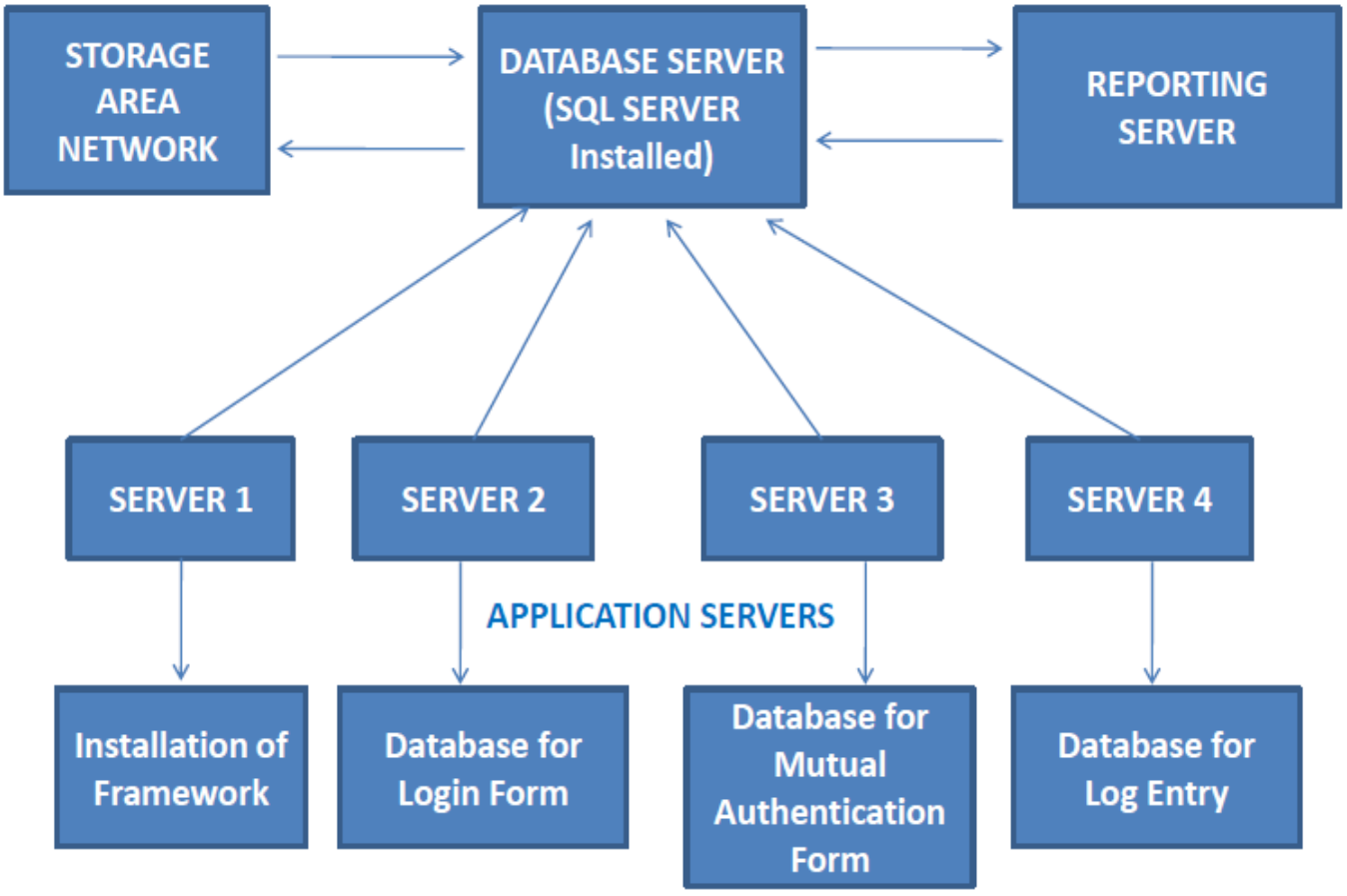

Figure 1: Implementation of the Framework in which RNA-FINNT is implemented for fingerprint identification

So there is a possibility of complete Network Security with the use of RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm) in the framework.

IV. CONCLUSION

Paper concludes that execution of RNA-FINNT in which the number of minutiae points is increased, results in the reduction of error percentage. Fingerprint extraction could be done with lot many other techniques also like:

- Standardized Fingerprint Model [8][9]
- Latent Fingerprint matching [10]
- Feature extraction for image authentication [11]

ISBN: 978-981-07-5461-7

But RNA-FINNT results in the reduction of number of angles and error percentage. In the framework RNA-FINNT implemented for fingerprint extraction is assimilated with the Password to generate an Ideal Password Authentication Scheme. As Password have high impact strategies [12] so an ideal password authentication scheme has password as one of the check for security. Client and Server side both are checked for security for proving complete security check. Transport Layer is enhanced with the implementation of Password and Fingerprint (RNA-FINNT Implemented). Validation of RNA-FINNT for error reduction enhances the later of network. Overall paper states that:

- RNA-FINNT resulted in the reduction of error percentage when the number of minutiae points is increased.
- RNA-FINNT is implemented in the Framework which has Password assimilation with the RNA-FINNT for generating an ideal password authentication scheme.
- Framework implementation is shown in the Case Study of Lovely Professional University; in which framework is implemented in the Application Servers and complete Database is derived for generating a Multi Server Environment.

Paper validates the overall reduction in error percentage and will result in fortification of transport layer security protocol.

References

[1] KULJEET KAUR AND Dr. G. GEETHA," Survey for Generating an Ideal Password Authentication Scheme Which Results In Fortification of Transport Layer Security Protocol," International Journal of Computer Science and Information Technologies, Vol.3, Issue.2, PP.3608–3614, March-April 2012 (http://www.ijcsit.com/ijcsit-v3issue2.php)

[2] KULJEET KAUR AND Dr. G. GEETHA. Article," Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters", International Journal of Computer Applications, 42(6):36-42, March 2012. Published by FCS,NY,USA.

[3] KULJEET KAUR AND Dr. G. GEETHA. Article," Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter", International Journal of Computer Science Issues,Vol.9, Issue.2, No.2, PP.188-193,March 2012.

[4] ATSUSHI SUGIURA, YOSHIYUKI KOSEKI, " A User Interface Using Fingerprint Recognition- Holding commands and Data Objects on Fingers-,"C & C Media Research Laboratories, NEC Corporation, Japan 1998.

[5] RAFFAELE CAPPELLI, DARIO MAIO, DAVIDE MALTONI, JAMES L. WAYMAN, ANIL K. JAIN," IEEE Transactions on Pattern Analysis and Machine Learning, Vol.28,No.1,January 2006.

[6] QIJUN ZHAO, LEI ZHANG, DAVID ZHANG, NAN LUO, " Direct Pore Matching for Fingerprint Recognition", Biometrics Research Center, Hong Kong 2009.

[7] KULJEET KAUR, Dr. G. GEETHA,"Framework for Proving Fortification of TLSP with IPAS", International Journal of Computer Engineering and Technology, Volume 3, Issue 2: 499-505, July-September, 2012.

[8] LE HOANG THAI, HA NHAT TAM," Fingerprint Recognition using Standardized Fingerprint Model", International Journal of Computer Science Issues, Vol.7, Issue 3, No.7, May 2010.

[9] JIANJIANG FENG, JIE ZHOU," A Performance Evaluation of Fingerprint Minutiae Descriptors", IEEE 2011.

[10] ANIL K.JAIN, JIANJIANG FENG," Latent Fingerprint Maching", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.33, No.1, January 2011.

[11] CHIN-CHEN CHANG, CHIH-CHIANG TSOU, YUNG-CHEN-CHOU," A remediable image authentication scheme based on feature extraction and clustered VQ," PCM'07 Proceedings of the multimedia 8th Pacific Rim conference on Advances in multimedia information processing, 2007(http://dl.acm.org/citation.cfm? id=1779525)

[12] GERARD BLOKDIJK," Password Management: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors", 2011 (http://www.scribd.com/doc/61409165/Password-Management-High-impact-Strategies-What-You-Need-to-Know-Definitions-Adoptions-Impact-Benefits-Maturity-Vendors)

About Author (s):

Asstt.Prof. Kuljeet Kaur is heading the domain of Systems and Architecture in the School of Computer Applications at Lovely Professional University, India. She is research scholar of PhD in Lovely Professional University, India. She has successfully implemented 5 projects. She has published 23 research papers in refereed Journals and Conferences. She serves as Reviewer in the International Journal of Research in Computer Science. She has attended 5 International Workshops and Faculty Development Programs. Her interest areas are Network Security, Identity Authentication and Systems Architecture. She is an active member of CSTA, ISCA, CSI and ISTE.

Prof.G.Geetha is heading School of Computer Science and Applications, Lovely Professional University, India. Her research interest includes Cryptography, Information security and Image Processing. She has published more than 50 research papers in refereed Journals and Conferences. She serves as Editorial Board member and reviewer in various Journals and Conferences. She is presently the President of Advanced Computing Research Society. She is an active member of various professional organizations like ISCA, ISTE, CRSI etc.