American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-09, pp-62-70
www.ajer.org

Research Paper Open Access

Smart input based user authentication and challenges towards multi-tiered cyber security

Ziaur Rahman, Md. Baharul Islam, A. H. M. Saiful Islam
[1]*(Department of ICT, Mawlana Bhashani Science & Technology University, Tangail-1902, Bangladesh)*
[2]*(Department of Multimedia Technology and Creative Arts, Daffodil International University, Bangladesh)*
[3]*(Department of Computer Science and Engineering, Daffodil International University, Bangladesh)*

Abstract: - Ever been a situation where a cyber crime investigation authority is searching for a convicted user who has allegedly done something illegal and the authority only can identify the system where from the crime is committed instead of having any information about the acquitted user exactly they are looking for. If we compare this scenario with our real world offenses that means the police has found the site where the crime is held but they have no idea or clue about the criminal. It should deserve a great concern that this type of thing is happening in our today's modern cyber world in each every day. We can easily find any system or network that is doing something offensive and fraud but it is not clear to us how we can find the acquitted user who has used that system to commit that fraud. We've tried to find a solution towards a sound solution of the problem we've been ever facing in our cyber world. In this paper we have proposed a smart input based user authentication method that can reduce online fraud in the cyber world.

Keywords: - *activity history, biometric devices, finger print pattern, feature noise, online security, smart button*

I. INTRODUCTION

Sensitive mouse or keyboard is not an unknown term. We're going to tell here a similar concept might not be much unknown. We do many activities in our daily life by using our computer system where basically we use Input / Output (IO) devices. For example if we want to surf internet we usually need to open a browser to write an address on address bar. For this we need an event generated by mouse or keyboard or by any device we ever have. Monitoring input can play a vital role especially when we're talking about monitoring our cyber world. In this paper we've proposed a new type of keyboard and mouse layout where ENTER key of the keyboard and RIGHT BUTTON of the mouse are sensitive or there is an extra input button on the input systems that is biometrically sensitive. That means when a user will enter an account using this key or button a special interruption will be sent to the client or server containing identifiable user information. Identifying information may vary from user's finger print, Retinal Scan Code, Iris Recognizer, Vein Pattern, Face Recognition Code, Iris Scan code, Hand or Leg Print Readable Code or geometry, Voice prints, Keystroke timing, Signature, Smart Passport Voice Analyzer to DNA mapping code analysis. Here we've used an input system what can only read the finger print of the user. To be more explicit is that in our research we've tested this type of smart input just using finger print scanning. When a user will press ENTER key or sensitive BUTTON to login into his account the smart input key or button will send that user's special information to the system through interruption.

II. BACKGROUND RESEARCH

One may ask why we're going to choose finger print technology inside the smart input device to identify the user. Fingerprint based authentication although sometimes not as high-profile as other high-tech crime-solving methods like DNA typing, is still very much used in criminal investigations and other fraud detection cases. Though the principle that no two persons could have the same fingerprints cannot be scientifically authenticated, fingerprint evidence is generally considered to be highly secure, reliable and is particularly accessible to juries. It doesn't need much talk to conceive that your fingers contain a map of ridges and whorls that is completely unique without any confusion. There are different types of classification as available at present all over the world. In the Henry system of classification, there are three basic fingerprint patterns. These are loop, whorl and arch. Loop constitutes 60–65%, whorl constitutes 30–35% and arch constitutes 5% of all fingerprints. Another complex systems used by most experts are similar to the Henry system of classification. In general, it consists of five fractions R, L, I, m, and t where R stands for right, L for left, i for index finger, m for middle finger, t for thumb, r for ring finger and p (pinky) for little finger. The fractions are as follows:

$$R_i/R_t + R_r/R_m + L_t/R_p + L_m/L_i + L_p/L_r$$

Because of its availability and development fingerprints are more useful because than DNA according to forensic experts say. In the last decade several papers published aimed at illustrating the intersection among biometrics devices, cryptographic system and so forth. David, et al. (1998) was among the first to suggest offline biometric authentication what was actually a PKI (Public Key Infrastructure) like environment with local fingerprint matching. The flaw was that it required local authentication. Then Fuzzy Commitment Scheme Juels et al. (1999) is encoded with the association of standard error correcting code such Hamming or Reed- Solomon and then XORed. Major problem of this system was that biometric data was often subject to reordering and erasures which cannot be handled using this scheme. Another strategy Nichols et al. (1999) was provided using the phase information of a Fourier transformation of the scanned image. The fingerprint information and a randomly chosen key are mixed to make it impossible to recover one without other. This was not address how much these steps reduce the entropy of the original images thus it was not clear that there exists a set of parameters which will allow the system to determine the legitimate users while providing a reasonable amount of security. In his paper Monrose et al. (1999) is item to add entropy to user's passwords on a computer system through data from the way in which they type their passwords. As biometric is being used so that radically different from fingerprints, their results are not applicable to the solution. Juels and Sudan (2002) proposed fuzzy commitment scheme, which is more compatible with partial and reordered data.

2.1. Fuzzy Vault

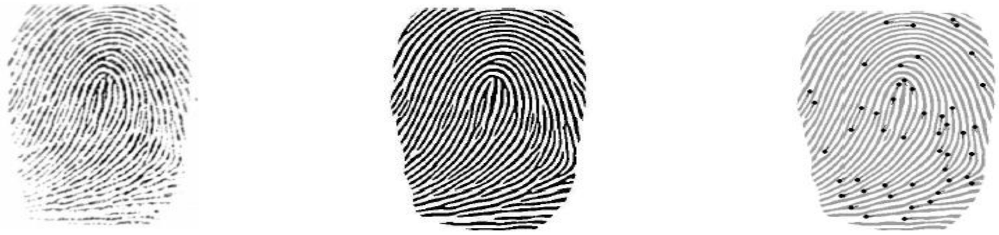
Let's see the original fuzzy vault, with some slight notational differences. As with any cryptosystem, there is some message m to be decrypted for that symmetric fuzzy key that could be used. Suppose the message *m* is first encoded as the coefficient of some degree *k* polynomial in *x* over a finite field $F_{q.}$. Here the polynomial f*(x)* needs to protect. Locking set *L* is a set of values $l_i \in \mathrm{F}_q$ making up the fuzzy encryption key, where $t > k$. The lock vault contains all the pairs $(l_i, f(l_i))$ and some large number of chaff points $(\alpha_j, \beta_{j)},$ where $f(\alpha) \neq \beta_j$. After adding the chaff points, the total number of items in the vault is *r*. In order to crack the system, an attacker must separate the chaff points from the legitimate points in the vault. The difficulty of this operation is a function of the number of chaff points, among other things. To successfully interpolate the polynomial an unlocking set *U* of *t* elements such that $L \cap U$ contains at least $k + 1$ element. Here *f(x)* is a degree *k* polynomial in $F_q[x]$, $t \geq k$ points in *L* interpolate through *f(x)* and $r \geq t$ is total number of points in the vault. This vault shall be referred to as $V\,(F_{q,}\, r,\, t,\, k)$.

2.2. Polynomial Interpolation

To reconstruct the secret locked within the fuzzy vault, the points in the unlocking set must be used to interpolate a polynomial. Usually using brute-force search polynomial could be recovered where $k + 1$ element subsets of the unlocking set are used to interpolate a degree *k* polynomial, using Newtonian Interpolation Hilderband (1956). Another method is to use Reed-Solomon decoder Massey (2003) as suggested Juels and Sudan. RS decoding algorithm could be categorized into two: the Berlekamp-Massey (1969) algorithm and the Guruswami-Sudan (1998) algorithm. Another field called noisy polynomial interpolation has some recent advances, notably by Arora and Khot (2002) and Bleichenbacher and Nguyen (2000).

2.3. Feature Extraction

The Feature extraction process Verifinger (2009) is visually represented in the following figure 1.



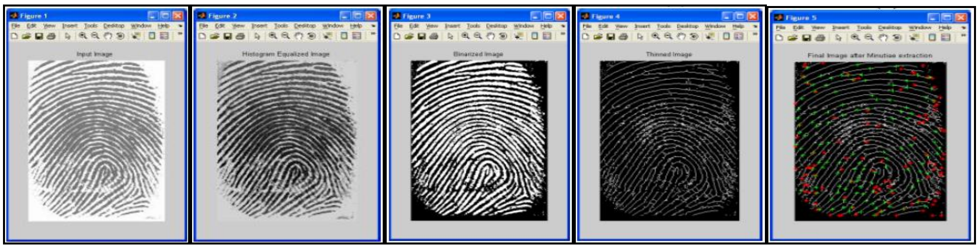
(a) (b) (c)

Figure 1: Feature Extraction Process: (a) Original Image (b) After Edge Detection, (c) Including Feature Points

In (a), image scan of a fingerprint is available which is received from the Fingerprint device. After applying different edge detection algorithms the information inside is converted into (b). And in the (c) the fingerprint *minutiae* the location where fingerprint ridge either splits or ends are shown. Here the black box is considered as feature extraction and alignment. This yields to normalized *(x,y)* pixel coordinates of minutiae.

2.4. Feature Noise

A typical print consists of a certain set of minutie locations $m_i = (x_i,y_i) \in M$. Because of errors in capturing, processing and aligning noise is added. In that case it seems like this equation. $m_i' = (x_i + n_{xi} , y_{i,+} n_{yi})$. If N sample images are taken from a person the result is a set of expected values ($\bar{x}_i$, $\bar{y}_i$) for every achieved minutiae. The number $n \leq N$ of samples of having a minutiae in that neighboring region. The variance and covariance of those n minutiae of those n minutiae ($\sigma^2_{x,i}$, $\sigma^2_{y,i}$, ρ_i). To get the geometrical spatial transformation (RST), let us consider an image function *f* defined in (w, z) coordinate system to get an image *g* over (x, y) Mehfuza Holia (2010).



(a) (b) (c) (d) (e)

Figure 2: (a) Original Image (b) Gray Scale Image (c) Binarized Image (d) Thinned Image (e) Final Minutiae

In the algorithm this RST transformation is applied on the each input fingerprint image to see how much it is rotated or scaled or translated with respect to the database image or the original image. In figure 12 (a) shows the original image, (b) shows the gray scale image, (c) shows the binary image, (d) shows thinned image and lastly (e) shows the final minutiae image. Two common features of the fingerprint image are ridge termination and ridge bifurcations Mandi (2012). Minutiae detection is a trivial task when an ideal thinned ridge map is available. After this result we will take any arbitrary point as reference point and align this to the origin. Then consider the shortest distances and find the relations as per considered two images. The Table 1 here shows FAR and FRR at different values. The summary is that FRR increases as threshold value increases, FAR decreases as threshold increases and at 0.023, they match each other. This is also known as Equal Error rate. In the table above GA stands for Genuine Accept.

Table I: False acceptance rate and False Rejection Rate

	TH-1	**TH-2**	**TH-3**	**TH-4**	**TH-5**
TH	0.01	0.017	0.023	0.03	0.04
FA	15	12	4	1	0
FA (%)	21.7	17.4	5.8	1.4	0.0
FR	0	0	4	22	29
FR (%)	0.0	0.0	5.8	31.9	42.0
GA	54	54	52	36	30
Accuracy	91.5	91.5	88.1	61.0	50.8

III. PROPOSED RESEARCH

User authentication consists of a computer verifying that you are who you claim to be. There are three main techniques:

- what you know
- what you have
- what you are

Biometric devices like our proposed smart input (fingerprint analyzers or biometric devices or even DNA code analyzer) almost fit into the last category. Actually our opinion is that if we confidentially can authenticate "who you are?" then anything else is almost optional. If these categories are combined together then the security will be multi-tiered security .This is done by adding smart input with the existing systems.

3.1. Research Environment

In our research plan we have done an experiment with a system consisting of sensitive mouse and keyboard. For this we have used SecuGenOptiMouse Plus Fingerprint Reader (Model MSDU03M2) and Keyboard (Microsoft Optical Desktop - MS BZ5-00002) as in Figure 3. Both Devices are USB portable and easy to use immediate after installing the respective software associated with it. SccuGenOptimouse is an optical mouse with an integrated ultra-fast, high performance fingerprint reader that holds three programmable buttons and let fingerprints act like a digital password.

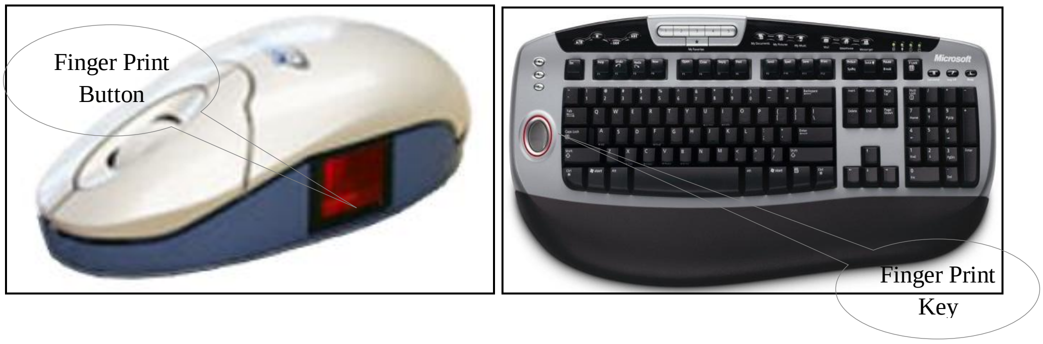


Figure 3: SecuGenOptiMousePlus Fingerprint Reader (Model MSDU03M2) and Microsoft Optical Desktop - MS BZ5-00002

We fetch the devices with the system and prepared the desired environment to work as a smart input system. After installing the necessary software for both devices we've connected the system the system with the internet. To test how the Smart Input works we will use a simple email system that we've titled as "Smart Input Email System" which we've already developed using some common API and PHP. This site is able to communicate with the sensitive devices connected with the system.

3.2. Hypothesis

Just like other typical biometric system our proposed smart input system has four basic units (as shown in the Figure 4) are Sensing, Storage, Signal Processing and Interface Unit. Sensing unit varies as the type of sensor device changes. We've applied optical sensor but Charged Coupled device (CCD), Complementary Metal Oxide Semiconductor (CMOS) or even Thermal or Pressure also could be applied. However, CMOS imager or CCD could be used for face, iris, retinal or leg or handprint recognition. Storage could be SDRAM or Flash which are connected to Digital Signal Processing (DSP) device. Here, the processing element is generally a microprocessor. But in another case digital signal processor, computer or any other similar device may be used. A programmable DSP from Texas Instrument® is suggested to use here for the better output. The purpose of the Storage Element is to store the enrolled template that is recalled to execute the matching operation at the time of authentication. Random Access Memory (RAM) or flash EPROM or some any other form of Integrated Circuit(IC) or even data server may be used. Finally, there is an output interface that will communicate the decision of the system to user. This could be general communication protocol like RS232 or the higher bandwidth USB portable protocol. Or even TCP/IP protocol using wired medium e.g 10/100 Ethernet or wireless medium or Bluetooth or any other cellular protocol could be used. In our experiment we suggest to use USB storage for smooth outcome.

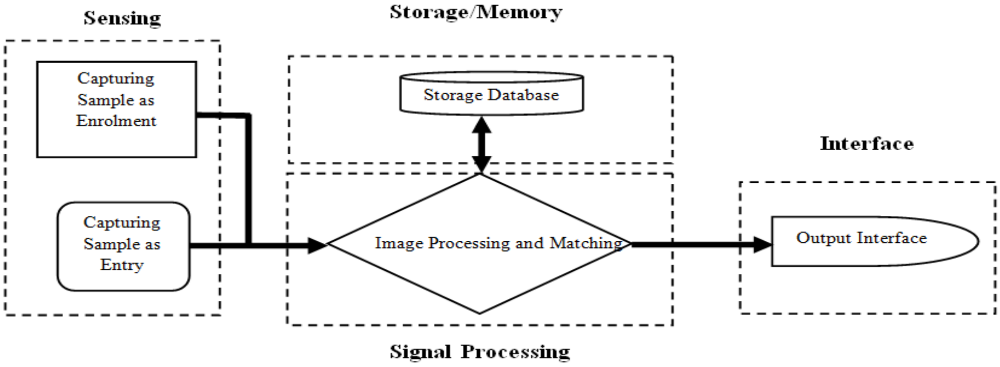
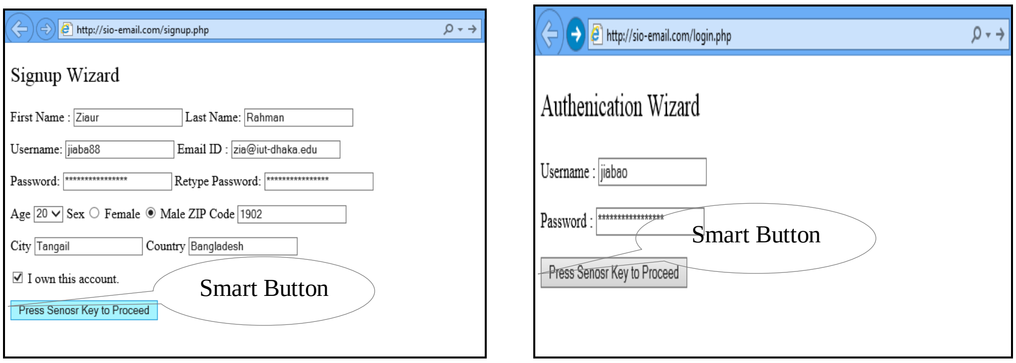

Sensing
Capturing Sample as Enrolment
Capturing Sample as Entry
Storage/Memory
Storage Database
Image Processing and Matching
Signal Processing
Interface
Output Interface

Figure 4: Working elements of fingerprint as smart input

IV. RESEARCH STUDY

First of all we need redirect the registration page which is known as Signup Wizard to create a new account. For registration we have to enter Name, Username, Password and others. Then we need to press the "Press Sensor Key to Proceed" button which we called smart button as a sample snapshot is shown in the Figure 5. While the user presses the Smart button (Fingerprint sensor key) the software will store his fingerprint code with other information



http://sio-email.com/signup.php

Signup Wizard

First Name : Ziaur Last Name: Rahman

Username: jiaba88 Email ID : zia@iut-dhaka.edu

Password: **************** Retype Password: ****************

Age 20 Sex ○ Female ● Male ZIP Code 1902

City Tangail Country Bangladesh

☑ I own this account.

Press Senosr Key to Proceed

http://sio-email.com/login.php

Authenication Wizard

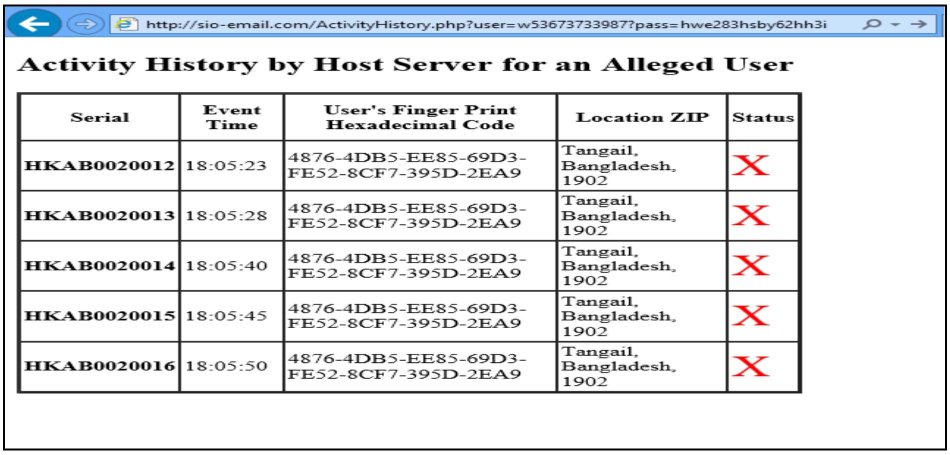
Username : jiabao

Password : ****************

Press Senosr Key to Proceed

Figure 5: Sample signup wizards to register into the site able to work and authentication wizard to login into the site using smart input

Then to login into the Email system we as usually need to authenticate our identity. For that, if we click on login tab available in the home page of the Email Page we'll be shown the window as shown in Figure 5. Here after entering the username and password we'll have to again press the Smart Key. This time it will validate user's entered information with the information which is stored in the Databases. If the information does match then we'll be given access to the email system otherwise access will be denied. If someone tried to login into the Smart Email Input System by entering the arbitrary username or password it could be caught easily by monitoring the Activity History generated by the host server. The host server where the Email system is hosted is able to generate this history automatically. To show this more precisely a snapshot of the Activity History Window is attached here in the Figure 6.



http://sio-email.com/ActivityHistory.php?user=w53673733987?pass=hwe283hsby62hh3i

Activity History by Host Server for an Alleged User

Serial	Event Time	User's Finger Print Hexadecimal Code	Location ZIP	Status
HKAB0020012	18:05:23	4876-4DB5-EE85-69D3-FE52-8CF7-395D-2EA9	Tangail, Bangladesh, 1902	✗
HKAB0020013	18:05:28	4876-4DB5-EE85-69D3-FE52-8CF7-395D-2EA9	Tangail, Bangladesh, 1902	✗
HKAB0020014	18:05:40	4876-4DB5-EE85-69D3-FE52-8CF7-395D-2EA9	Tangail, Bangladesh, 1902	✗
HKAB0020015	18:05:45	4876-4DB5-EE85-69D3-FE52-8CF7-395D-2EA9	Tangail, Bangladesh, 1902	✗
HKAB0020016	18:05:50	4876-4DB5-EE85-69D3-FE52-8CF7-395D-2EA9	Tangail, Bangladesh, 1902	✗

Figure 6: Activity History of an alleged user auto generated by the Host Server

V. CHALLENGES

Fingerprinting critics level three main arguments. First, fingerprint examiners have not established objective and proven standards for evaluating whether two prints "match." Second, the error rate for fingerprinting as a technique has been inadequately studied. Third, there is no statistical foundation for assessing the likelihood that two people might have prints with any given number of corresponding characteristics. This lack of statistical foundation is especially troubling in cases involving distorted and smudged fingerprints. We will examine each argument in more detail. The first claim is that fingerprint examiners in the United States have not developed uniform standards for determining what counts as a sufficient basis for an identification. In some countries, fingerprint examiners require a certain number of "points of identification" before declaring a match; England, for example, requires sixteen such points, while France requires twelve.

2.5. Finger Print Accuracy Rate

One of the important Challenges is the accuracy. Calculations of accuracy of finger print extraction with the system are

- False Acceptance Rate (FAR): The fault where someone of user which don't enlist will be held true by System. An Equation to express FAR is given below.

$$\mathrm{FAR} = \sum_{n=1}^{N} \frac{\mathrm{FAR(n)}}{\mathrm{N}} \qquad (1)$$

- False Rejection Rate (FRR). The fault when someone which registered in the system was refused by system.

$$\mathrm{FPR} = \sum_{n=1}^{N} \frac{\mathrm{FPR(n)}}{\mathrm{N}} \qquad (2)$$

- Failure to Enroll (FTE). A fault when system fail to enlist a new user ID:

$$\mathrm{FTE} = \sum_{n=1}^{N} \frac{\mathrm{FTE(n)}}{\mathrm{N}} \qquad (3)$$

- Equal Error Rate (EER) and Failure to Acquire (FTA) also could be calculated following the same way.

It is a challenge to understand the relationship between False Rejection Rate (FRR) and False Acceptance Rate (FAR) errors Frost and Sulliva (2000). For a system if the match score threshold is set lower, the FRR goes down and FAR goes up. There is a always a way out to represent this relationship using a plot FRR versus FAR on a Receiver Operating Characteristic (ROC) curve as shown in the figure below. Here in the figure above FRR affects usability and convenience, while FAR represents a security risk.

2.6. Finger Print Unlocking Complexity

In case of complexity of Valid User the objective is to minimize the complexity. But as per considered the complexity of an Attacker we always wish to increase the complexity as if an attacker cannot crack the vault. Two general ways could be applied for unlocking the vault. Brute-force method, or *bf(r,t,k)*, where r denotes total number of points, t for number of real points and k is the degree of the polynomial. For an attacker r, t are the same but for the valid user, r is the size of their unlocking set and t is the number of non chaff points. The respective theorem is that the complexity of the *bf(r,t,k)* problem using a suitable δ to ensure a unique result is-

$$C_{bf} = \binom{r}{\delta}\binom{t}{\delta}^{-1} \qquad (4)$$

This illustrates that a brute-force decoding algorithm is less than ideal a valid user.

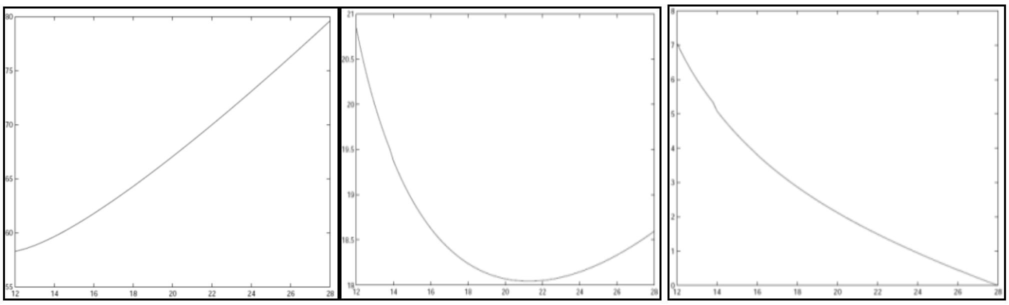


Figure 7: Log of Complexity for Reed Solomon decoding as a function of codeword size;(a)Complexity of full attack, rs (995, 40, n, 11); (b) Complexity of Partial information attack, rs(120, 40, n, 11);(c) Complexity of legitimate unlocking rs(31, 22, n, 12)

Another approach to unlock the vault is the use of Reed-Solomon decoder. In *rs(r, t, n,δ)* problem, r,t and δ have the same meaning as it had before whereas n is the size of the Reed-Solomon codewords involved. In that case the theorem is got the fashion below. The complexity of the *rs(r, t, n,δ)* problem over F_p^2 is

$$C_{rs} = \binom{r}{n}\left(\sum_{i=\max\left(\frac{n+\delta}{2},n-r+t\right)}^{\min(n,t)} \binom{r-t}{n-i}\binom{t}{i}\right) \text{ such that}$$

$$n \text{ satisfies } \delta \le n \le \min(r, 2t-\delta) \text{ and } (n|p^2-1) \qquad (v)$$

The MATLAB simulation of Reed Solomon Complexity of different scans is shown below.

2.7. Two Fingerprints Logistic Integration Challenges

Let $I_i(x_i)$ and $G_i(x_i)$ be the imposter and genuine distributions of the ith matcher, $i = 1, 2$. x_1 and x_2 are considered as the output scores. If we use logistic transform of two fingerprints matching and the logistic regression to $\hat{\pi}(x)$, the estimate will be

$$\pi(x): \log it\{(\hat{\pi})\} = (\alpha + \beta x_1 + \gamma x_2) \qquad (6)$$

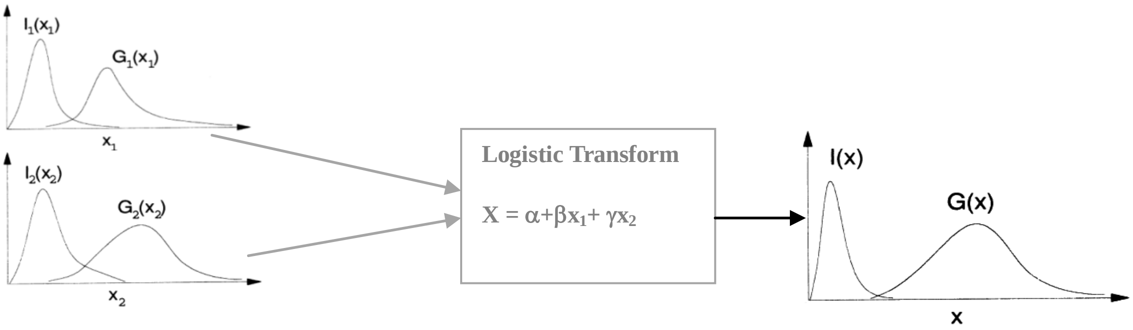


Figure: 8. Integration of two fingerprint matching algorithms using a logistic transform with tunable parameters α , β and γ

Here,

$$x = l(\alpha + \beta x_1 + \gamma x_2 \qquad (7)$$

$$= \frac{\exp\,(\alpha+\beta x_1 + \gamma x_2)}{1+(\alpha + \beta x1 + \gamma x2)} \qquad (8)$$

Here α, β and γ three parameters The objective of the integration is to estimate the parameters such that the FRR is minimized for specified level of FAR. Let x_1 and x_2 are independent, the joint imposter and genuine distributions $I_i(x_i)$ and $G_i(x_i)$, respectively could be expressed as

$$I_i(x_i) = \iint I_1(x_1) I_2(x_2)\, dx_1\, dx_2 \qquad (9)$$

and

$$G_i(x_i) = \iint G_1(x_1) G_2(x_2)\, dx_1\, dx_2 \qquad (10)$$

Therefore, the new probability distribution functions I(x) and G(x) of imposter and genuine individuals, respectively, after logistic transform, can be written as

$$G(x) = \iint I_1(x_1) I_2(x_2)\, \delta(\alpha + \beta x_1 + \gamma x_2 - l^{-1}(x))\, dx_1\, dx_2 \qquad (11)$$

and

$$G(x) = \iint G_1(x_1) G_2(x_2)\, \delta(\alpha + \beta x_1 + \gamma x_2 - l^{-1}(x))\, dx_1\, dx_2 \qquad (12)$$

Here δ(.) is the delta function. In other words I(x) and G(x) are line integrals of $I(x_1,x_2)$ and $G(x_1,x_2)$,respectively along the line $\alpha+\beta x_1+\gamma x_2 = l^{-1}(x)$ on the (x_1,x_2) plane. The FRR, p_{frr} for a given α , β and γ and FAR, t_{far}, is

$$p_{frr}(\alpha, \beta, \gamma, t_{far}) = p_{frr}(t) = \int_{-\infty}^{t} G(x)\,dx \qquad (13)$$

Where

$$t = \arg_x \ \inf_x \{p_{frr}(x) \ge t_{far}\} \qquad (14)$$

$$= \arg_x \inf_x \{ \int_x^{+\infty} I(x)\,dx \ \ge p_{frr} \} \qquad (15)$$

And

p_{frr}(t) and t_{far}(t) are the FRR and FAR levels at the threshold t.

The integration of two fingerprints matching algorithms can be formulated as follows. For specified FAR levels$t_{far}^{(i)}$, i= 1, 2…, L compute the set of parameters (α_i , β_i, γ_i, t_i) which satisfy the following optimization criterion:

$$(\alpha_i, \beta_i, \gamma_i, t_i) = arg\ \min_{\alpha,\beta,\gamma}\left\{p_{frr}\left(\alpha, \beta, \gamma, t_{far}^{(i)}\right)\right\} \tag{16}$$

And,

$$t_i = \arg_x\ \inf_x \left\{p_{far}(x) \geq t_{far}^{(i)}\right\} \tag{17}$$

$$t_i = \arg{}_x \inf_x\left\{\int_x^{+\infty} I(x)dx \geq t_{far}^{(i)}\right\} \tag{18}$$

The minimization criterion estimates parameters (*α_i , β_i, γ_i, t_i)* such that the FRR is minimized at each given FAR level. Here the challenge is that as we do not know the analytical form of *I(x)* and *G(x)*, it is not possible to solve the minimization problem analytically. But in this Equation $(\alpha_i, \beta_i, \gamma_i, t_i) = arg\ \min_{\alpha,\beta,\gamma}\left\{p_{frr}\left(\alpha, \beta, \gamma, t_{far}^{(i)}\right)\right\}$ minimization may be solved using efficient algorithms.

VI. CONCLUSION

Using Fingerprint as a mean of smart input could bring better outcome comparing with other biometric ways existing today. But the fingerprint technique we are using nowadays has some security challenges. Some of the important drawbacks are discussed here in this paper, many of those are not. However, towards a secure and sustainable cyber world we certainly should use a security technique that is easy to use and available to all considering costs, complexities and other factors. Answering the security question in user authentication is basis of user privacy. But the username, password and so called capthca have some threats that we've already realized while we use theses. Beside this existing authentication technique if we add smart input technique then the security check will be multi-tiered and more trustworthy. Here in our continuous research work we suggest using this type of smart and sensitive key will be a very good solution towards multi-tiered online and cyber security.

REFERENCES

[1] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation, 18(2)*, 1998, 112-116.

[2] Arora, S., and Khot, S. 2002, Fitting algebraic curve to noisy data, ACM Symposium on Theory of Computing, STOC 2002

[3] Bellare, M., Canettiy, R., Krawczyk, H., (1996), Keying Hash Functions for Message Authentication, Advances in Cryptology, Vol. 1109, Springer-Verlag

[4] Bergman, P., Berman, S., *The Criminal Law Handbook: Know Your Rights, Survive the System.*

[5] Blahut, R. 2003 *Algebraic Codes for data Transmission* Cambridge University Press

[6] Bleichenbacher, D., and Nguyen, P. Q. 2000, Noisy polynomial interpolation and noisy Chinese remaindering. Advances in Cryptography, EUROCRYPT 2000

[7] Clancy, T.C., Kiyavash, N. and D. J. Lin, D. J. 2013 Secure Smartcard-Based Finger Print Authentication

[8] Coklin, Gardner, B. and Shortelle, D. 2002, Encyclopedia of Forensic Science: a Compendium of Detective Fact and Fiction. Westport, Conn. : Oryx, 2002, Print.

[9] Davida, Frankel, Y., and Matt, B., (1998), On enabling secure applications through off-line biometric identification. IEEE Symposium on Privacy and Security

[10] Frost and Sullivan, A Best Practices Guide to Fingerprint Biometrics http://www.frost.com

[11] Guruswami, V., and Sudan, M. 1998, Improved decoding of reed-solomon and algebraic geometric codes. Symposium on Foundations of Computer Science, FOCS1998

[12] Hildebrand, F. B. 1956, Introduction *to Numerical Analysis.* McGraw-Hill

[13] Kaufman, C., Perlman, R., Speciner, M. *Network Security: Private Communication in a Public World,* Second Edition.

[14] Jain, A. K. Prabhakar, S., Chen, S. Combing multiple matches for a high security fingerprint verification system

[15] Juels, A., and Sudan, M 2002, A fuzzy vault scheme. ACM Conference on Computer and Communication Security, CCS.

[16] Juels, A., and Watenberg, M., (1999), A fuzzy commitment scheme, ACM Conference on Computer and Communications Security

[17] Kekre, H. B. Sudeep D. 2012, Thepade, Dimple Parekh, Comparison of Fingerprint Classification using KFCG Algorithm with Various Window Sizes and Codebook, International Journal of Computer Applications, pp 0975-8887, Volume 46-No.17.

[18] Massey, J. L. 1969, Shift register synthesis and bch decoding. *IEEE Transactions on Information Theory vol. 15*, no. 1, pp. 122-127.

[19] Mandi, R. M., Lokhande, S. S. 2012 Rotation-Invariant Fingerprint Identification System, International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 2 Issue 4

[20] Miao, D., Tang, Q and Fu, W. 2007, Fingerprint Minutiae Extraction Based on Principal Cures, the Journal of the Pattern Recognition Letters, vol. 28, pp. 2184-2189

[21] Mehfuza, H., Thakar, V. K., 2010, Image registration for recovering affine transformation using Nelder Mead Simplex method for optimization.

[22] Morrose, F., Reiter, M., and Wetzel, S (1999), Password hardening based on keystroke dynamics. ACM Conference on Computer and Communication Security

[23] National, R. C., (2002), Cyber security Today and Tomorrow: Pay Now or Pay Later, National Academy Press, Washington, D.C.

[24] Nichols, R. K., (1999) Ed. *ICSA Guide to Cryptography*. McGraw-Hill, Chapter, Biometric Encryption

[25] Oliveira, L. B., Kansal, A., Priyantha, B., Goraczko, M., Zhao F., (2009), Secure-TWS: Authenticating Node to Multi-user Communication in Shared Sensor Networks, 8th International Conference on Information Processing in Sensor Networks, (IPSN'09), April 13–16, 2009, San Francisco, California, USA.

[26] Ritter, M. 2001, Fingerprint Evidence Faces Hurdles, FDIAI News

[27] Singhai, N 2010, '*A Survey on: Content Based Image Retrieval Systems*', International Journal of Computer Applications (0975-8887) Vol 4, No. 2, pp. 22-26.

[28] Smeulders, AWM 2000, '*Content based image retrieval at the end of the early years',* IEEE Transactions on pattern analysis and machine intelligence, pp. 1349-1380.

[29] Veringer 2013, Neurotechnologija Ltd. http://www.nurotechnologija.com