Fingerprint Authentication Security:
An Improved 2-Step Authentication Method with Flexibility

A. Q. M. Sala Uddin Pathan, Kamlesh Kumar Thakur, Abhijit Chakraborty, Mohammad Humayun Kabir

Abstract— we started this paper to continue the trend of Fingerprint Biometric Authentication System by making it more secure, robust and flexible. Despite the vast research by the scientists in the field of improving the recognition of the fingerprints, little is known about the viewpoint of flexibility for authentication. We went through more than 30 papers, and the overall image that emerges from the literature is that even if there are sufficient studies on improving fingerprint matching, we believe the flexibility part has not been touched as much as it deserved. An analysis of these studies motivated us to develop an advanced and effective model. The proposed solution which we came up with is based mainly on the fingerprints to prove the users' identity whether the user is approved or not. The idea is to store the fingerprints of more than one finger and combine each fingerprint with a secure password. The password consists of the fingers' sequence in hand plus a secure password. We were immensely satisfied with it, and it showed that this model is intense and challenging to break, and besides it provides the flexibility criteria that we were looking to address in the first place.

Index Terms— Fingerprint, 2-Step Authentication, Biometric Authentication, Flexibility, Security, Challengeing to break, Robust.

1 Introduction

Designing a complete system based on fingerprint recognition and the idea of providing flexibility by storing more than two fingerprints to ensure authentication in situations where a user is not able to authenticate himself due to the problems in one of the fingers (like simple cuts, bandages in the thumb). Moreover, 2 step authentications achieved by using unique passwords for each finger.

1.1 Motivation and Challenges

Every organization either government or private, educational or high security physical has to maintain proper authentication record of the users or make sure that a user does not have access to something s/he is not authorized; meanwhile it also has to ensure that the legitimate ones get access to where they have been allowed. Now, consider the situations where there are thousands of users working in an institution and one of the users had a pure accident and had managed to injure a finger or even a hand. The same finger or hand's finger s/he used to authenticate himself/herself. The institution may not have a dedicated user or branch to handle these kinds of situations, and the concerned user will be in a spot of bother. Designing a better system for users so that they can authenticate themselves with ease and accuracy was an essential key behind motivating this project. Moreover, as the processing power of the machines increases day by day, several methods invented to break the latest password methods as well as biometrics like the fingerprint. Therefore, combining both fingerprints and passwords using a unique password for each of the finger in the hand will provide 2-step authentication with the flexibility to use any finger for the authentication process.
This would pretty much tackle all the situations when users are not being able to authenticate themselves due to the problems described in the above paragraph and will, in turn, improve the security of the overall system. We made sure the fingerprints matching time does not exceed the reasonable limit by searching for only that finger's fingerprints in the database which is entered by the user.

1.2 Using Biometrics

Biometric Authentication Systems are widely used for unique identification of humans mainly for verification and identification purpose. Biometrics can be used for identity access management and access control. There are many types of biometric systems like fingerprint recognition, voice recognition, iris recognition, palm recognition, etc. The analysis of our study presented the fact that we can't provide flexibility to other biometric systems as much as we can do in the fingerprint system. Therefore, the use of a fingerprint biometric system in our paper is evident.

1.3 What is a Fingerprint?

Human fingerprint shows some specific details marked on it; a fingerprint is the pattern of valleys and ridges on the surface of a fingertip. Fig 1.3.1 illustrates a sample fingerprint image created by a friction ridge structure. The endpoints and crossing points of the ridges are known as minutiae, which can be used as a unique identifier of a person if we recognize it suitably. It is accepted the assumption that the minutiae pattern of each finger is unique and does not change during one' lifetime. Ridge curve terminates at ridge endings. Bifurcations are where a ridge splits at a Y-junction from a single path to two paths.

Fig 1.3.1: A fingerprint created by the friction ridge structure
Source: Wikipedia

The example of a ridge ending, and a bifurcation is shown in Fig 1.3.2. In this example, the white pixels correspond to the valleys, and the black pixels correspond to the ridges. When checking the fingerprints to determine if two fingerprints are from the same finger, the matching degree is the most critical

factors. The application of fingerprints has evolved immensely. Nowadays, we use fingerprints for various purposes like, to note down daily attendance, criminal science, authenticate into high security physical and forensic investigation.

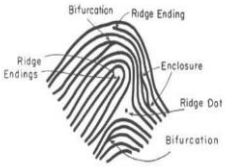

Fig 1.3.2: An example of a ridge ending and a bifurcation
Source: H. Chang, D, 1999

1.4 Why use Fingerprints?

Fingerprints are considered to be the fastest and best method for biometric authentication. They are secure to use and unique for every person as no two people have been found to have the same fingerprints – they are unique, and it also does not change in one's lifetime. Now to present an idea of how unique a fingerprint is, there is one in 64 billion chance that a fingerprint will match up exactly with someone else's [1]. Fingerprints are even more unique than DNA. Though identical twins can share the same DNA – or at least the most of it – they can't have the same fingerprints [2]. Besides these, the implementation of the fingerprint recognition system is easy, cheap, and accurate up to a satisfactory level. Fingerprint recognition has been used in both civilian and forensic applications. Compared with other biometrics, fingerprint-based biometrics is the most proven technique and has occupied the large portion of the market. The global market for Fingerprints Biometrics is projected to reach US$11.9 Billion by 2020. According to a survey [3], the financial service industry is more likely to use fingerprints (31% to be exact) than other biometric modalities.Newer trends like cloud biometrics will ease the affordability of the biometric. Frost and Sullivan estimated that market revenue for fingerprint authentication on mobile devices would increase from US$52.6 million in 2013 to US$396 million in 2019 [4].

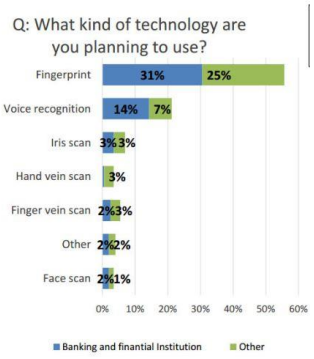

Fig 1.4.1: Results of a survey conducted by Mobey Forum in 2015 [3]

2 Current research on Fingerprint

Feng and Jain [5] proposed a novel approach to fingerprint reconstruction from minutiae template which reconstructs a phase image from the minutiae template and then converts the phase image into the greyscale image. The benefits of this approach over existing approaches to fingerprint reconstruction [6], [7], [8] are: (i) a complete fingerprint can be reconstructed and (ii) the reconstructed fingerprints contains very few spurious minutiae. Seung-hwan Ju et al. [9], [10] introduced a better authentication methodology that combines numeric-based password and biometric-based fingerprint authentication system. The first research was solely based on password-based authentication system whereas the second research paper merged the password-based authentication system with fingerprint biometric information. Further, this research said that the password authentication systems currently used are easy, but if it gets leaked somehow then user authentication is vulnerable. Using the fingerprints, only the user with the information which is specific to the authentication security is strong. Here are some problems such as the user cannot change the authentication key. Hence no flexibility is achieved. As the fingerprint cracking methods are developing rapidly, we should focus more on security.

3 The changing Fingerprint breaking Landscape

The fingerprint is the most popular biometric characteristics due to its uniqueness and persistence of friction ridge pattern [11]. Investigation of spoofing attacks on the fingerprint system has not been as a concern as their market has grown. Finding the vulnerabilities and fixing them in a fingerprint system is a natural research area for the researcher [12]. Finding new vulnerabilities helps the system to improve continually [13]. To design secure systems, we should implement the latest threats to see if there are any vulnerabilities and develop a mechanism to protect the system against that. Most of the sensor devices use a small window for a finger to collect data. As a result, a small part of our fingerprint is saved in the database. As it is not possible to place the same part of the finger in the sensor device every time, devices take multiple reading for a single fingerprint. If we have n fingers in the system and if each finger has m readings, then there are n x m possibilities for a match. That's why a partial fingerprint can easily be matched with another partial fingerprint of different fingers. Roy et al. [14] introduced Master-Prints, a combination of real or synthetic fingerprints using a hill-climbing procedure on partial fingerprints, which can be used to match with a large number of fingerprints. It shows the vulnerability of a fingerprint-based security system. By using this method, one can easily spoof a subject without knowing his fingerprint. Roy et al. [14] demonstrated that Master-Prints were generated by modifying the minutiae points in a fingerprint [15]. But it was not practically possible to generate an image from this method. Analysing this issue, Bontrager et al. [16] generated an image-level Master-Prints called Deep-Master-Prints by training a Generative Adversarial Network (GAN) which has more accuracy than other methods. Variational Autoencoders (VAE), Fully Visible Belief Networks (FVBN), and Generative Adversarial Networks (GAN) are some popular methods for image generation [17]. GANs use an unsupervised learning method to generate an image by using a generator and a discriminator. GANs trained the discriminator for the classifica-

tion of a real image by providing real images to it. Then it feeds generated images to it for the classification of a generated image. The generator also being trained to produce real images. These processes are repeated to complete the actual data distribution. Bontrager et al. [16] demonstrate, for generating images instead of minutiae, templates have one advantage to develop Deep-Master-Print for any fingerprint system that accepts images [18]. Attacks can be launched at the sensor level by transferring the images to a spoof artefact. It uses a single fingerprint to match with different fingerprints by combining with a method of searching. It also uses evolutionary optimization to search the latent variable space of the neural network for a Deep-Master-Print. It can spoof 77% of the subjects in the dataset for 1% FMR and 23% of the subjects for 0.1% FMR.

Smartphones become the focus of attack due to their small sensors. Forecast demonstrates that 50% of smartphones will have a fingerprint sensor by the end of 2019 [19]. Cao et al. [20] presented an effective method for spoofing the fingerprint sensor in a mobile phone using a 2D fingerprint image printed on a special paper. This spoof fingerprints have been generated automatically. They scanned the target fingerprint-image at higher resolution (approximately at 300 dpi). To achieve this task, AgIC4 silver conductive ink cartridges along with black ink cartridge in an inkjet printer for printing the original or binarized fingerprint-image after mirroring, have been used. These 2D fingerprints are to be used for spoofing sensor devices. Galbally et al. [21] executed different experiments on a fingerprint database and showed that over 75% of the attempts were granted by the system which is highly vulnerable to the proposed attack scheme. Thus, the belief of minutiae templates non-reversibility has been disproved and raises a key vulnerability issue in the use of non-encrypted standard templates. Cappelli et al. [22] and Ross et al. [23], demonstrated that a digital image similar to original fingerprint could be reconstructed from a minutiae-based fingerprint template which has enough information. This image can be used for spoofing a biometric system. It was compared to the original fingerprints and injected the reconstructed images into the feature extractor. Cappelli et al. [22] and Ross et al. [23] described an algorithm to reconstruct images similar to the original fingerprint from its ISO minutia-based template. Galbally et al. [21] performed a systematic and replicable evaluation of a more dangerous security threat: transforming such an indirect attack into a direct attack. The reconstructed images were used to make gummy fingers. The success chances of such attack are evaluated on a standard and publicly available fingerprint database [24], using a competitive matching algorithm working with ISO/IEC 19794-2 templates [25]. Ratha et al. [26] discussed the possibility to generate fake biometric samples in order to access a system illegally and defined it as the first vulnerability point in a biometric security system. Putte et al. [27] examined the vulnerability of several sensors to fake fingerprints made with plasticine and silicone. Different methods to create gummy fingers were classified into two main categories: with and without the cooperation of the original user. One method of each class was described, and the possibility of breaking different commercial sensors was explored on a yes or no basis. Matsumoto et al. [28] carried out similar experiments to those reported in [27], this time with fake fingerprints made of gelatin. Again, they distinguished between the case in which they had the cooperation of the fingerprint owner (five different fake fingerprints were generated this way) and the situation in which the latent fingerprint had to be lifted from a surface (just one gummy finger of this type was used in the experiments). Galbally et al. [29] presented the first statistically significant evaluation of two different fingerprint verification systems against direct attacks. (Only fake fingerprints generated with the cooperation of the user were considered). We took motivations from the new trends and proposed our new system.

4 METHODOLOGY

4.1 System Design

Fingerprints are ridge and furrows patters on the tip of the finger [30] and have been used extensively for personal identification of human [31]. The fingerprint is a state of art security measure as compared to password and other conventional security methods. Both the fingerprint and password security is used to design a more secure and efficient security system where the user can authenticate himself with any of the fingerprints which they have provided earlier. Reading of the fingerprints is beginning with the left hand from the pinkie finger which will be stored as "1" and as it goes to the thumb whose location will be "5". For the right hand, the location of the thumb will be "6", and so on until we reach the pinkie finger in the right hand whose location will be "10". Fig 4.1.1 shows the password fingerprint.

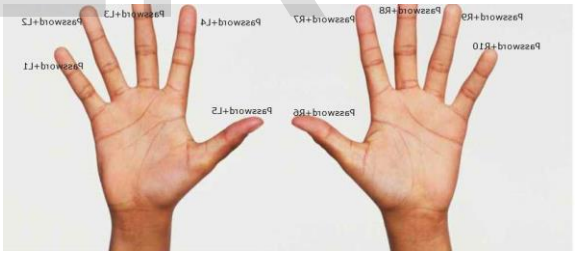

Fig 4.1.1: Fingerprint Password Model

User have to provide at least two finger's fingerprint or all ten finger's fingerprints for this system. Now when the fingerprints have been submitted, the user is required to enter the password for the fingerprints which is again asked to enter twice for the confirmation. Now the thing to be careful with is that when we save the password for the fingerprints, the password is saved against all the fingerprints provided by the user separately and automatically. That means, the user only has to enter a single password. However, we will generate passwords for each of the fingerprint provided by the user automatically, and each password will be different from others as we will save the passwords according to the finger's position and the fingerprint position number, which will be added at the end of each of automatically generated passwords. Now, an obvious question here would be, how can a user remember ten passwords (even though we are likely not

going to use all the fingerprints, we are just making it more flexible by taking all ten fingerprints or the number of fingerprints provided by the user) when most people have the problem remembering one. The issue of memorizing the passwords is resolved by putting one password accompanied by the location of the finger so that they will be remembered enthusiastically. This way is considered to be effective and it provides us multiple passwords that are easily remembered by the authorized user but will be very difficult to memorize by an unauthorized one.

For example, suppose the user enters the fingerprints for the Right thumb, Right index and Right pinky and password he enters is My@Password. Now the things will happen and where we will generate three passwords for each of the fingerprints provided by the user. Consequently, to produce all the passwords automatically and uniquely at the same time what we will do is that we add the location of the finger at the end of the password provided by the user. That is, for the Right thumb the last password will be My@PasswordR6, in the same way, the password for the Right index will be My@PasswordR7 and finally for the Right pinky the password that will be saved in the database will be My@PasswordR10. This is how we can achieve unique passwords for all the fingerprints, and it will also help the user to remember passwords easily. The point to keep in mind that when the user enters the fingerprint and its corresponding password, the password the user has to enter is the password with the location of the finger at the end of it. For Example, if the user enters his Right thumb's fingerprint for verification, then correct password that the user has to enter has to be My@PasswordR6. This is how the login process will cycle in. The user can choose any fingerprint he had provided earlier at the time of signing up for the account and its corresponding password with the correct location of the finger.

4.2 Fingerprint Authentication System: GUI User Manual

We have divided the overall system into two parts — one where we have presented the steps in matching the password and another where the fingerprint matching steps are described. Since our design and simulation is in MATLAB, so we have used Matlab coding to implement this task. The steps used in the method are as follows.

I) First of all, a collection of passwords, fingerprints are saved in the database along with the details of the user.

II) When a user wants to enter the system, he must enter the username and password to get access.

III) After the username and password are entered properly, it is matched with the already stored usernames and passwords in the database.

IV) If the entered username and password matches with any of the stored usernames and passwords combination in the database then "Username logged in successfully message" dialogue box appears.

V) For the incorrect username and password, a message will be displayed saying "Username/Password does not match" and access is not granted to the user. If the username matches successfully but the password does not match with the corresponding username which matched earlier then "Password does not match" message is displayed.

The working procedure of full system showed through different figures in the following section.

a) First of all, a GUI appears which offers two options whether to Login into Server and to check About Developers as shown in Fig 4.2.1. When the user clicks on About Developers, a new GUI appears which shows the details of the developers.

Fig 4.2.1 Starting GUI

b) When the user presses on the Login into Server, a new GUI appears asking the user to enter username and password as shown in Fig 4.2.2. Now this GUI also offers two options to the user. If the user already has an account, then he can directly enter the username and password which was provided to him during his account creation. Now if the user does not have an account, what he can do is to sign up for a new account and then he can have his username and password for after the sign-up process is successful.

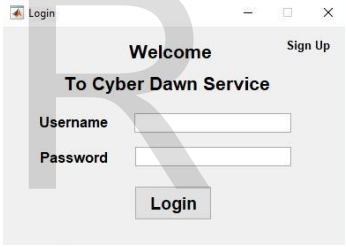

Fig 4.2.2: Login GUI

In case of a new sign up the GUI that appears is presented in Fig 4.2.3. In this GUI form, the user will provide some of the details, a photo of him along with his desired username and password. Now the username must be unique. The user will get a notification if he tries to use a username

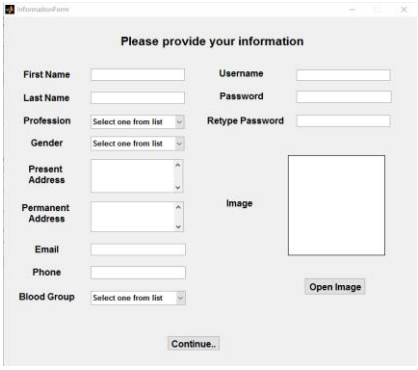

Fig 4.2.3: Sign Up GUI

that already exists. Furthermore, we have asked the user to enter the password in two separate fields for the confirmation. If the passwords entered in both the areas do not match then, the user will be notified and hence will be asked to re-enter the passwords again.

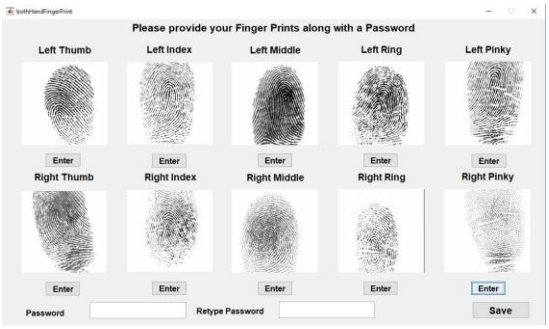

Fig 4.2.4: Fingerprints Submission GUI with provided fingerprint

After the user enters the details required in Fig 4.2.3 and when clicking on Continue does not result in an error, then a new GUI appears where the user has to register the fingerprints. User, at least, have to enter fingerprints of more than two fingers and if he wishes, then he can provide fingerprints of all the ten fingers of the hand. Now when the fingerprints have been submitted, the user is required to enter the password for the fingerprints which is again asked to enter twice for the confirmation. When the user presses on Save, all the details that he had entered in the GUI Fig: 4.2.3 and in GUI Fig 4.2.4 is saved in the database if no further error appears. Now the thing to be careful with is that when we save the password for the fingerprints, the password is saved against all the fingerprints provided by the user separately and automatically. That means, the user only has to enter a single password. However, we will generate passwords for each of the fingerprint provided by the user automatically, and each password will be different from others as we will save the passwords according to the finger position number and the fingerprint position number will be added at the end of each of automatically generated passwords.

c) If the user already has an account, then the user will enter the username and password in their respective fields as shown in Fig 4.2.2 Login GUI. Then after pressing on Login, if the entered username and password match with any of the stored usernames and passwords combination in the database then "Username logged in successfully" message dialogue box appears. If the entered username and password does not match with any of the stored data in the database, then a message is displayed saying "Username/Password does not match," and access is not granted to the user. If the entered data are matched in the database or in another way if the login is successful, then a GUI appears asking the user to submit the fingerprint and the corresponding password for that fingerprint which is shown in Fig 4.2.5.

Fig 4.2.5: Submit Fingerprint and Corresponding Password for Verification GUI

d) After the fingerprint is submitted by the user and its corresponding password when the user clicks on submit. The user entered fingerprint, and its corresponding password is matched with the database and if the match is found a new GUI is presented with welcoming the user with his username, his photo and the match percentage as shown in Fig 4.2.6.

Fig 4.2.6: Welcome GUI

The point to keep in mind that when the user enters the fingerprint and its corresponding password, the password the user has to enter is the last password that was saved in the database, i.e., password with the location of the finger at the end of it. For Example, if the user enters his Left thumb's fingerprint for verification, then correct password that the user has to enter has to be My@PasswordL5. We presented our proposed solution for making the overall authentication system more secure, robust and flexible and discussed the approach of the system.

5 Conclusion

In this paper, we have combined biometric and conventional, i.e., a password security system and we have also proposed to keep more than two fingerprints of the user each having separate secure passwords. The current password security has several advantages as well as disadvantages. Those disadvantages have been overcome by using the fingerprint security system. The flexibility issue which we wanted to address has been solved by storing more fingerprints of the user's fingers. So overall, the system has the advantages of the biometric and conventional security system and flexibility to authenticate which makes it more potent than either of the two security measures working alone. We have also taken appropriate steps to improve the fast response time and accuracy.

References

[1] Stephanie Watson, "How Fingerprint Works" [Online], Available: http://science.howstuffworks.com/ fingerprinting1.htm, Access date: 9 December 2018.

[2] "Why Identical Twins Have Different Fingerprints?" [Online], Available: https://www.sciencefocus.com/the-human-body/why-do-identical-twins-have-different-fingerprints/, Access date: 9 December 2018.

[3] Mobey forum [Online], Available: https://www.mobeyforum.org/, Access

date: 9 December 2018.

[4] Global Biometric Market Analysis: Trends and Future Prospects [Online], https://www.bayometric.com/global-biometric-market-analysis/

[5] J. Feng, and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," IEEE Trans. PAMI, vol. 33, no. 2, pp. 209-223, Feb. 2011.

[6] C. Hill, "Risk of masquerade arising from the storage of biometrics," Master's Thesis, Australian National University, 2001.

[7] A. Ross, J. Shah, and A.K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," IEEE Trans. PAMI, vol. 29, no. 4, pp. 544-560, Apr. 2007.

[8] R. Cappelli, et al., "Fingerprint image reconstruction from standard templates," IEEE, Trans. PAMI, vol. 29, no. 9, pp. 1489-1503, Sep. 2007.

[9] Seung-hwanJu, Hee-suk Seo, "Password-based user authentication methodology using multi-input on multi-touch environment," Korea simulation academy Vol. 20, No. 1, pp. 39-49, 2011.

[10] Seung-hwan Ju, Hee-suk Seo, Sung-hyu Han, Jae-cheol Ryou, and Jin Kwak, "A study on user authentication methodology using numeric password and fingerprint biometric information," Hindawi Publishing Corporation BioMed Research International vol. 2013, article ID 427542, Aug. 2013.

[11] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Second Edition, Springer, 2009

[12] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614–634, 2001.

[13] E. Marasco and A. Ross. A survey on anti-spoofing schemes for fingerprint recognition systems. ACM Computing Surveys, 47(2):1–36, 2015.

[14] A. Roy, N. Memon, and A. Ross. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Transactions on Information Forensics and Security, 2017.

[15] A. Roy, N. Memon, J. Togelius, and A. Ross. Evolution-ary methods for generating synthetic masterprint templates: Dictionary attack in fingerprint recognition. In International Conference on Biometrics, pages 1–8, 2018.

[16] P. Bontrager, A. Roy, J. Togelius, N. Memon, A. Ross. "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution." arXiv preprint arXiv:1705.07386, 2018.

[17] I. Goodfellow. NIPS 2016 tutorial: Generative adversarial networks. arXiv preprint arXiv:1701.00160, 2016.

[18] Apple. iOS Security - White Paper, 2017.

[19] Market Research, [Online]. Available: http://www.marketresearch.com/Research-Capsule-v4026/Fingerprint-Sensors-Smart-Mobile-Devices-8918844. Access date: 24 November 2018.

[20] K. Cao and A. K. Jain, "Hacking Mobile Phones Using 2D Printed Fingerprints", MSU Technical Report, MSU-CSE-16-2, 2016.

[21] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct attacks using fake fingers generated from ISO templates. Pattern Recognition Letters, 31(8):725–732, 2010.

[22] Cappelli, R., Lumini, A., Maio, D., Maltoni, D., 2007b. Fingerprint image reconstruction from standard templates. IEEE Trans. PAMI 29, 1489–1503.

[23] Ross, A., Shah, J., Jain, A.K., 2007. From template to image: Reconstructing fingerprints from minutiae points. IEEE Trans. PAMI 29, 544–560.

[24] Fierrez, J., Ortega-Garcia, J., Torre-Toledano, D., Gonzalez-Rodriguez, J., 2007. Biosec baseline corpus: A multimodal biometric database. Pattern Recognition 40, 1389–1392

[25] ISO/IEC 19794-2, 2005. Information Technology – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data.

[26] Ratha, N., Connell, J., Bolle, R., 2001. An analysis of minutiae matching strength. In: Proc. AVBPA. LNCS, vol. 2091. Springer, pp. 223–228.

[27] Van der Putte, T., Keuning, J., 2000. Biometrical fingerprint recognition: Don't get your fingers burned. In: Proc. IFIP, pp. 289–303.

[28] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, H., 2002. Impact of artificial gummy fingers on fingerprint systems. In: Proc. SPIE, vol. 4677, pp. 275–289.

[29] Galbally, J., Fierrez, J., Rodriguez-Gonzalez, J.D., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M., 2006. On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In: Proc. IEEE ICCST, vol. 1, pp. 130–136.

[30] H. C. Lee and R. E. Gansslen (editors), "Advances in Fingerprint Technology," Elsevier, New York, 1991.

[31] A. K. Jain, L. Hong. S. Pankanti, and Ruud Bolle, "An identity authentication system using fingerprints," Proceedings of the IEEE, vol. 85, no. 9, pp. 1365-1388, 1997