International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 6, June - 2014

Secure Authentication Approach for Human using Finger Images

Ms. Monali S. Khonde
ME, Student, Dept. of Electronics & Telecommunication
PVPIT, University of Pune,
Pune, India

Prof. S. M. Kulkarni
Dept. of Electronics & Telecommunication
PVPIT, University of Pune,
Pune, India

***Abstract*— Nowadays, authentication is a major concern in security. This paper presents a new approach to improve the performance of finger-vein identification systems. The sharing or theft of user passwords still remains the most frequent way that corporate data is compromised. This proposed system obtains the finger vein and finger texture and merge these two evidences using a novel score level combination. This paper examines previously proposed finger- vein identification approaches and develops a new approach to illustrate its superiority over prior published efforts. This new system also supports the utility of low resolution finger print images acquired from a camera is examined to determine the matching performance from such images. This paper investigates and develops two new score-level combination i.e. holistic and nonlinear fusions, and also comparatively evaluating them with other popular score-level approaches to establish their effectiveness in the proposed system.**

***Index Terms*—Finger-vein recognition, feature extraction, Personal Identification, Fusion (Holistic and Nonlinear).**

I.INTRODUCTION

Automated human identification such as biometrics that uses human physiological or behavioral features for verification, has increasingly mapped for commercial use and also tremendously demands for more user-friendly and secured biometrics [1] has motivated researchers to explore new biometrics features and traits. For decades, the password has been widely considered as standard means for user verification on computers. However, as users are required to memorize and changing the passwords, it is essential that a more suitable and safe solution to user authentication is needed. For many researchers it is a challenge to find out a highly secured authentication technique using biometrics. So they have sought to improve the consistency and annoy spoolers by developing biometrics that are highly individuating [2]. The individuality of fingerprints has been recognized to the casual imperfections in the friction ridges and valleys. The acquisition of such minutiae features typically requires imaging resolution higher than 400 dpi. The convenience of such features acquired from the low-resolution (webcam) images or at a distance [4], deserves attention for its feasible use in personal identification for particular applications.

Some biometrics technologies are liable to satire attacks in which fake fingerprints and static face images can be effectively employed as biometric samples to imitate the identification. Hence, several liveness counter measures to detect such sensor-level spoof attacks have been proposed [1], [10], e.g., finger response to electrical impulse [5], finger temperature and electrocardiographic signals [6], time-varying perspiration patterns from fingertips [7], and a percentage of oxygen-saturated hemoglobin in the blood [8].

II. MOTIVATION AND RELATED WORK

The principle behind the finger vein authentication technique is as follows: The pattern of blood vessels is caught by transmitting near infrared light and light is partially absorbed by hemoglobin in the veins and the pattern is caught by the webcam. The finger-vein patterns are believed to be quite unique, even in the case of identical twins. There are two factors that are cited for the preference of finger-vein biometrics. 1) The finger veins are concealed structures hence complicated to steal the finger-vein patterns of an any person without their awareness.2) It offers robust antispoofing capabilities as it can also guarantee liveness in the presented fingers during the imaging.

Finger vein detection is a method that utilizes pattern-recognition techniques based on finger images of human finger vein patterns beneath the skin's surface of the finger to identify individuals identity. To obtain the pattern for the database record, the person has to insert a finger into an attester terminal including a near-infrared LED and a CCD camera. The CCD camera records the finger image and the raw data is digitized and sent to a database of stored registered images.

II. PROPOSED SYSTEM

The fingers presented for the identification of subjects are simultaneously exposed to a webcam and an infrared camera, as illustrated from the device of our imaging device in Fig. 2(a). The dorsal side of a finger is exposed to the near-infrared frontal surface illuminators, using light-emitting diodes whose illumination peaks are at a wavelength of 850 nm, whereas the frontal surface entirely remains in the contactless position with both of the imaging cameras. The finger-vein and finger texture images are simultaneously acquired using the switching device/ hardware that can switch the infrared illumination at a fast pace.

The obtained finger-vein and finger texture images are first given to preprocessing steps, which automatically extract the region-of-interest (ROI) images while reducing the translational and rotational variations. The enhanced and normalized ROI images are employed to extract features and then generate matching scores similar with a conventional biometrics system. The combined matching scores are employed to authenticate the user.

Fig 1. Represents the block diagram of the system and its blockwise explanation is as given below:

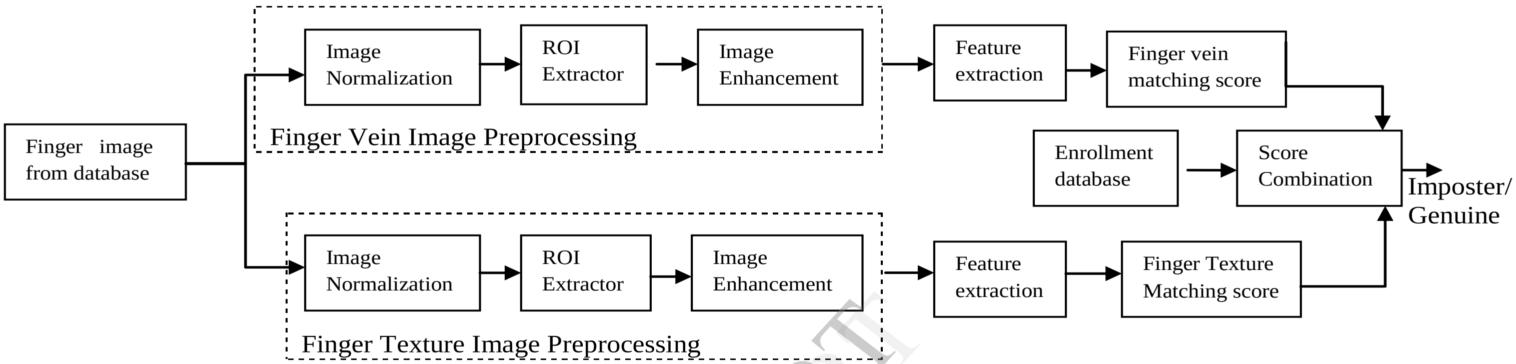
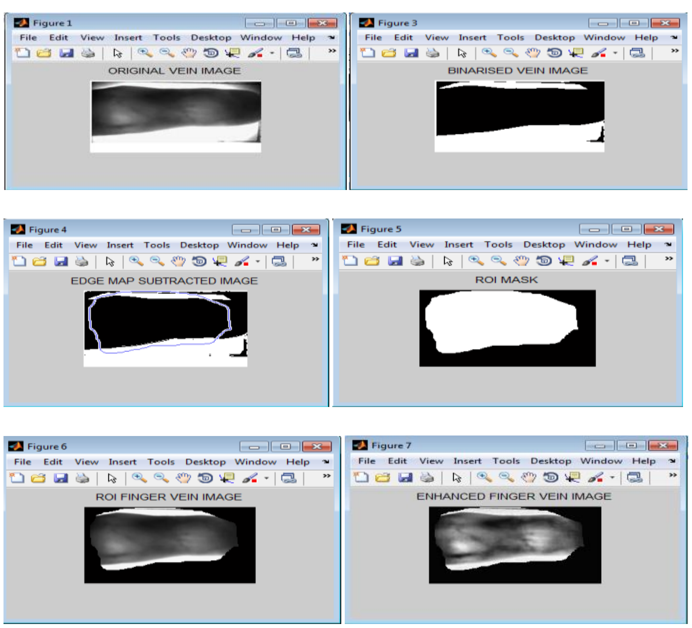


Fig 1. Block diagram of the proposed system

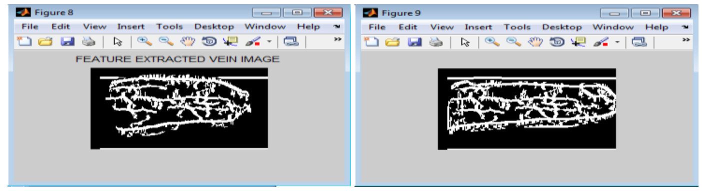
A. FINGER-VEIN IMAGE PREPROCESSING

The acquired finger images are noisy having rotational and translational variations resulting from unconstrained imaging. Therefore, the acquired images are first subjected to preprocessing steps where it includes 1) Image Normalization 2) ROI extraction 3) Image Enhancement



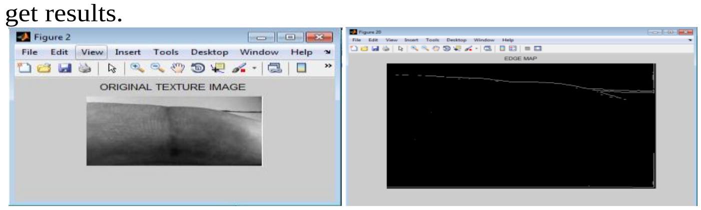
B. FINGER-VEIN FEATURE EXTRACTION

The normalized and enhanced finger-vein image from the imaging setup represents a vascular network with varying thickness, clarity, and uncertainty on the topological connections.



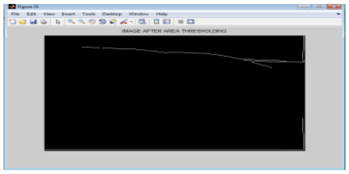
C. FINGER TEXTURE IMAGE PREPROCESSING

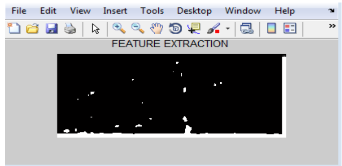
The obtained finger texture images from the webcam (640x480 pixels) are compact to 580 x380 pixels gray-level images because the cropped part does not supply any useful finger details. Then this image is employed for the preprocessing and get results.



D. FINGER TEXTURE IMAGE FEATURE EXTRACTION

The localized Radon transform (LRT) and the Gabor-filter-based extraction of such localized texture orientation details have shown to propose promising outcome for the identification of finger knuckles and palmprints.





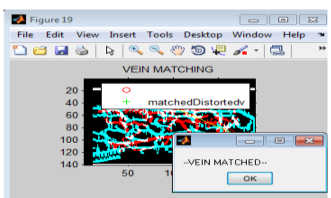
E. GENERATING COMBINED MATCHING SCORES

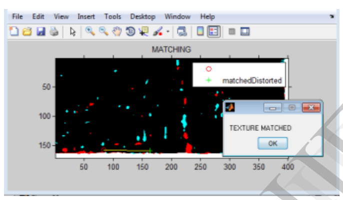
The combination strategy selected or developed should be robust and achieve significant performance improvement. These all output results can be combined at the feature, score, and decision levels.

This approach searches for the linear combination that can provide the best separation of the genuine and imposter scores in the decision space and can be represented as follows:

$$\hat{S} = \sum_{j=1}^{L} (w_j \times s_j), \text{ where } \sum_{j=1}^{L} w_{j=1}$$

Where s_j represents the scores from the jth matcher, w_j denotes the weight that is assigned to the jth matcher (computed from the training data), and is the combined matching score.





III. EXPERIMENTAL WORK AND RESULTS

The real glory of finger vein authentication is its versatility. Because of its small and highly manageable size, it can be used for everything from gate-access control units to currency machines; car doors to PC log ins. In the future, it could even be used on portable electronic devices like cell phones and MP3 and also be adapted for identity documents like driving licenses, ID cards or passports.

Here the two main approaches are used such as: First, a new approach for personal identification that utilizes simultaneously acquired finger-vein and finger surface (texture) images is presented. Second, this paper investigates two new score-level combination approaches, i.e., holistic and nonlinear fusion, for combining finger-vein and finger texture matching scores. We comparatively evaluate the proposed fusion approaches with the sum, average, product, weighted sum, likelihood ratio, and Dempster–Shafer fusion.

.

- . *Holistic Fusion*

This approach is developed to utilize the earlier knowledge in the dynamic combination of matching scores. Let Sv , S t , and η represent the matching score from finger vein, finger texture, and combined score, respectively, and this holistic rule of score combination is illustrated as follows:

$$\hat{S} = \{(Sv*\eta)+(St*(1-\eta))\} + \frac{\{(Sv*\eta)+(St*(1-\eta))\}}{(2-Sv)}$$

$$= \{(S\upsilon*\eta)+(St*(1-\eta))\} + \{(1+\frac{1}{2-S\upsilon})\}$$

The final combined scores have a similar trend as the score from vein matching, when the score from finger-vein matching is high, the fused score will also become high and vice versa.

- *Nonlinear Fusion*

The nonlinear fusion score combination tries to dynamically adjust the combined score according to the degrees of uniformity between the two matching scores and is illustrated in the following:

$$\hat{S} = (\frac{c+St}{c+Sv})^{\gamma} * (c+Sv)^2$$

Where c is a positive constant and is fixed to 1 in this experiments and γ is selected in the range of [1, 2]. As the equation suggests, when the two matching scores are consistent, the final combined score is primarily contributed by the vein matching score.

Finally after comparing both finger vein and finger texture it will generate the output as data stored in the database. It is shown by both software and hardware .The message will be displayed on the LCD display as match founds and simultaneously relay will be on the LED glows.

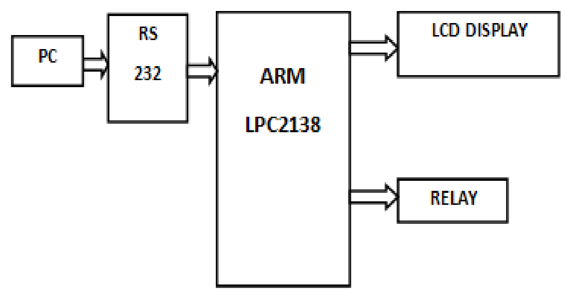


Fig. 2 Circuit diagram of Hardware

Fig. 2 shows the circuit diagram which is used as output. Where the output of software is given as input to the hardware relay circuit through RS232. If the vein and texture match founds then only the relay will be ON and message will be displayed on the LCD. If the match is not found then the relay will not get ON.

The 10 database images are taken to generate the result on the basis of vein matching score, texture matching score, Equal error rate holistic, holistic fusion matching, Equal error rate non-linear, non linear fusion matching . All the statistics are shown in following table by precision.

Sr. no.	Vein Matching Score	Texture Matching Score	EEHR	Holistic Fusion Matching	EERN	Non-Linear Fusion Matching

1	0.929962	0.17	1.211	98.789017	1.5907	98.409328
2	0.928609	0.21	1.2396	98.760393	1.6839	98.316131
3	0.922782	0.29	1.2913	98.708666	1.8758	98.124222
4	0.869624	0.23	1.1568	98.843243	1.7154	98.284602
5	0.91940	0.23	1.2249	98.775092	1.7267	98.273316
6	0.924962	0.22	1.2411	98.758925	1.7066	98.293374
7	0.906962	0.21	1.2028	98.79719	1.6782	98.321835
8	0.914699	0.31	1.2928	98.707242	1.9231	98.076946
9	0.925789	0.17	1.2039	98.796125	1.5896	98.410361
10	0.918684	0.25	1.2534	98.74655	1.7768	98.223161

Fig.3 Table shows statistics of matching

IV. CONCLUSION

This finger-vein matching technique works more efficiently in realistic scenarios and leads to a more precise performance, as demonstrated from the experimental results. Beyond embedded applications for portable IT devices such as cellular phones, finger vein authentication will in the future likely expand into applications such as opening automobile doors with a simple grip of the handle, for which the necessary grip-type authentication technology is already in development. Grip-type technology embeds personal authentication in the natural motion of opening a door, ensuring the highest security without forcing the user to learn complicated new procedures. This technology will be applicable to home, office or car doors and will usher in a secure future without keys.

V. REFERENCES

[1] Encyclopedia of Biometrics, S. Z. Li, Ed.. New York: Springer-Verlag, 2009.

[2] D. Wang , J. Li, and G. Memik, “User identification based on finger vein patterns for consumer electronics devices”, IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 799-804, 2010.

[3] A.K. Jain, Y. Chen, and M. Demirkus, “Pores and ridges: High resolution fingerprint matching using level 3 features,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 1, pp. 15–27, Jan. 2007.

[4] Handbook of Remote Biometrics, R. Chellappa,M. Tistarelli, and S. Z. Li, Eds. New York: Springer-Verlag, Jul. 2009.

[5] P. Kallo, I. Kiss, A. Podmaniczky, and J. Talosi, “Detector for recognizing the liveness character of a finger in fingerprint recognizing apparatus,” U.S. Patent 6 175 641, Jan. 16, 2001.

[6] D. Osten, H. M. Carin, M. R. Arneson, and B. L. Blan, “Biometric personal authentication system,” U.S. Patent 5 719 950, Feb. 17, 1998.

[7] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, “Time-series detection of perspiration as a liveness test in fingerprint devices,” IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 35, no. 3, pp. 335–343, Aug. 2005.

[8] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, “A new antispoofing approach for biometric devices,” IEEE Trans. Biomed. Circuits Syst., vol. 2, no. 4, pp. 328–337, Dec. 2008.

[9] Finger Vein Products Aug. 2010 [Online]. Available: http://www.hitachi.co.jp/products/it/veinid/global/products/index.html

[10] A. Antonelli, R. Capelli, D. Maio, and D. Maltoni, “Fake finger detection by skin distortion analysis,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 360–373, Sep. 2006.

[11] Z. Liu, Y. Yin, H. Wang, S. Song, and Q. Li ,“Finger vein recognition with manifold learning”, Journal of Network and Computer Applications, vol.33, no.3, pp. 275-282, 2010.

[12] E. C. Lee and K. R. Park, “Restoration method of skin scattering blurred vein image for finger vein recognition,” *Electron. Lett.*, vol. 45, no. 21, pp. 1074–1076, Oct. 2009.

[13] D. Mulyono and H. S. Jinn, “A study of finger vein biometric for personal identification,” in *Proc. ISBAST*, Islamabad, Pakistan, 2008, pp. 1–8.

[14] L. Wang, G. Leedham, and S.-Y. Cho, “Minutiae feature analysis for infrared hand vein pattern biometrics,” Pattern Recognit., vol. 41, no. 3, pp. 920–929, Mar. 2008.

[15] A. Kumar and K. V. Prathyusha, “Personal authentication using hand vein triangulation and knuckle shape,” IEEE Trans. Image Process., vol. 18, no. 9, pp. 2127–2136, Sep. 2009.

[16] J.-G.Wang,W.-Y. Yau, A. Suwandy, and E. Sung, “Person recognition by palmprint and palm vein images based on ‘Laplacianpalm’ representation,” Pattern Recognit., vol. 41, no. , pp. 1531–1544, 2008.