Identification of Merged Bio-cryptic Patterns using Bio-Pattern Recognition Algorithm in Security Levels of Wireless Local Area Network

Ajay Babu Moparthi
Dept of Computer Science and Engineering,
Swarnandhra College of Engineering and Technology,
JNTUK, West Godavari, A.P, India

Sudhakar Godi
Dept. of Computer Science and Engineering,
Swarnandhra College of Engineering and Technology,
JNTUK, West Godavari, A.P, India

Rajasekhara Rao Kurra
Department of Computer Science and Engineering,
Sri Prakash College of Engineering, Tuni, Andhra Pradesh, India

ABSTRACT

Authentication module plays a vital role in securing wired or wireless network from intrusion attacks. Especially Wireless Networks (WN) are more prone to the security threats. This paper discusses in strengthening the authentication process of Wireless Local Area Network (WLAN) by recognition of various levels of Wireless Authentication Packets (WAP). The WAP comprises of diverse combinations of Bio-cryptic merged patterns like thumb-print, Iris, Palm-print and face. WAP is used in accordance with the security level. In general, the biometric pattern matching algorithm is used to match the patterns individually. But in WLAN, the Advanced Radius Authentication Server (ARAS) comprises of Merged Bio-cryptic pattern matching and identification is a challenging task for the practitioners and investigators. To resolve the above issue, this work proposes a novel Bio-Pattern Recognition (BPR) Algorithm for the effective recognition of the Bio-cryptic patterns. The proposed algorithm was compared with the existing each individual recognition algorithm. Where reliability, recognition time, True Positive Identification Rate (TPIR) and False Negative Identfication Rate (FNIR) were considered as major parameters. Finally the experimental results show the overall performance of the proposed BPR algorithm is better in patter recognition with respect to the recognition time.

General Terms

Wireless communications, Pattern recognition and Security.

Keywords

Bio-Cryptography, Bio-pattern recognition algorithm, Quality-of-Security, ASPS, SPSS, Biometrics, Security Level, Enhanced Merged Bio-cryptic Security- Aware Packet Scheduling-Algorithm, Bio-cryptic Security-Aware Packet Scheduling-Algorithm, BSPS, EBSPS,MMBSPS, BPR Algorithm.

1. INTRODUCTION

Wireless Network plays an important life in the normal day-to-day life, because of its extensive applications. Wireless Networks can be categorized into Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN), Wireless Mesh Networks (WMN), Wireless Metropolitan Area Networks (WMAN), Global Area Netwroks (GAN),Cellular Networks (CN) and Space Networks (SN). Wide variety of applications are available in the market depending on the type of network and demand [1][2][3]. For instance, applications like Push-to-talk and WiMAX operated on WMN [4][5], Whereas Global System for Mobile Communications and Digital Advanced Mobile Phone Service etc. are based on CN. Also WLAN has many such applications like Campus-connect and other WiFi usages [6]. This paper is more concern about, WLAN and its security. Due to the Information and communication Technology wide spread usage WLAN gain more popularity. But the protection and preservation of data in WLAN is a bold challenge for the scholars and scientists. Especially more criticality is involved in authentication modules in WLAN. Many researchers have proposed various types of solutions to strengthen the authentication process using pure Biometric, Bio-cryptic and merged Biometric-cryptic templates. ARAS based various algorithms use these methodologies in the authentication process. Among such algorithms Enchanced Merged Bio-cryptic Security aware Packet Scheduling (EMBSPS) and Multi-Merged Bio-cryptic Security aware Packet Scheduling (EMBSPS) drawn more attention by using the merged bio-cryptic templates[7][8]. In EMBSPS and MMBSPS the bandwidth is reduced and improved the communication between the ARAS and Wireless Node. But the algorithms did not address, the identification errors in the ARAS. Error identification broadly classified into True Positive Identification Rate (TPIR) and False Negative Identification Rate (FNIR) to the merged Bio-cryptic patterns. ARAS authentication depends upon pattern identification based on RSA encryption[9]. Many researchers proposed various methods on automatic pattern recognition algorithms, but the Sparse based face recognition algorithm is a robust method for the pattern detection [10]. Further the algorithms are discussed in the next section.

This paper verifies the EMBSPS security level authentication method correctness. This paper will test all the merged biometric image security levels without encryption to the biometric templates. The major benefication of the paper is as follows: (1) a study and analysis of biometric authentication in Wireless Local Area Networks through pattern matching; (2) a Sparse solution based Bio-Pattern Recognition (BPR) Algorithm; and (3) a new performance by combining both TPIR and Security Level; (4) a working model simulator where the BPR algorithm was developed and tested. The rest of the paper is structured is as follows. Related works discussed in Section 2 in the area of WLAN security, Biometric applications, and pattern recognition algorithms. Section 3 describes the proposed solution and BPA algorithm. Experimentation and outcomes are discussed in Sections 4. In section 5, the work concluded with brief advantages and disadvantages of BPA with further scope.

2. RELATED WORKS

The present work is carried on EMBSPS based Equal-half-merging technique [7]. At each level the biometric images are merged together, which will reduce the packet size and improve the transmission speed. Many researchers have worked out on biometric authentication individually, but merged biometric authentication templates is the still a major limitation. Tsai-Yang Jea et al proposed a novel method for the partial fingerprint matching, but the matching includes brute force, there many heavy complexities involved in it [11]. Whereas D Zhang and team discussed on the palm-print recognition system, the work is based on holistic and local feature based approaches [12]. Majority of works was not concentrated with the partial palm print. Robust Iris recognition methods were successfully attempted by the R Chellepa et al., but the work didn't work with the partial iris data [13]. The iris matching algorithm is based on sparse based representations. Whereas John Wright et al implemented the sparse based face recognition system and tested well [10]. The matching technique is really faster and accurate. The security level concept is introduced in many WLAN by various researchers. But the practitioners are more concern about the encryption rather than matching, the details can be found in the security level and WLAN literature [14][15][16][17][18][19].

The patterns have concentrated only on But the majority of algorithms is executed on a complete distinct biometric template individually. But the proposed BPR algorithm is used for recognition of partially merged biometric templates. The BPR algorithm uses Divide-and-conquer approach. The algorithm designation is discussed further in the section.

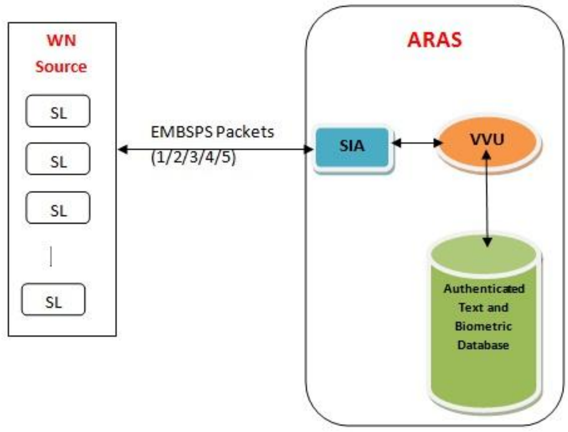


Figure 1: Proposed architecture for BPR algorithm

3. THE BIO-PATTERN RECOGNITION (BPR) ALGORITHM

The BPR algorithm is designed for the testification for the Equal-half biometric pattern recognition. The rest of the algorithm is shown below.

3.1 Assumptions and Notations

BPA algorithm assumes various of parameters like Security Levels (SL), FNIR and computation time. In the figure 1, only a limited security level of 5 were assumed and the Security Identfication Adapter (SIA) is used for assiging SL and granting the permission to access destination Wireless Node. SIA is based on Verification and Validation Unit (VVU). VVU is intermediary between SIA and Biometric database. It will perform all computation regarding the pattern matching. The BPR algorithm is incorporated in VVU. The EMBSPS all the request and response packets are assumed to communicate between Advanced Radius Authentication Server (ARAS) and Wireless Node with Network traffic with Uniform distribution function.

Where SL and FNIR is assumed using the Random Probability Distribution function. Whereas the total computation time of the Robust face recognition system is designated as:

$$\hat{\boldsymbol{w}}_1^{(l)} \doteq \arg \min_{\boldsymbol{w} \in \mathbb{R}^{n+p}} \|\boldsymbol{w}\|_1 \qquad \text{-------- (1)}$$

Subjected to

$$\left[A^{(l)}\ I\right]\boldsymbol{w} = \boldsymbol{y}^{(l)}.|$$

Where, $\bar{\boldsymbol{w}}^{(l)}$ is the sparse recovers and A is the matrix with l partitions with a x b block size. The computation is described in the reference[10].

3.2 The BPR algorithm

The Bio-Pattern recognition algorithm adopts EMBSPS network architecture and Sparse based Robust Biometric template authentication. The step-by-step representation are as follows:

Step1: Once the EMBSPS packet received at SIA in ARAS, with all authentication credentials,

```
IF SL2 GOTO Step2,
 ELSEIF SL3 GOTO Step3,
ELSEIF SL4 GOTO Step4,
ELSE Step5.
```

Step2: Packet data or credentials are forwarded to Verification and Validation Unit (VVU), where the Thumbprint biometric image is subjected to Sparse based Robust matching template in association with Biometric Database.

```
IF 'Thumprint' == 'Detected' GOTO Step6
ELSE Step7.
```

Step3: Packet data or credentials are forwarded to Verification and Validation Unit (VVU), where the biometric image separated accordingly and Sparse based Robust matching is applied to the Partial-Thumbprint and Partial-Iris templates in association with Biometric Database.

```
IF 'Partial-Thumprint' == 'Detected' && 'Partial-Iris' == 'Detected'GOTO Step6
ELSE Step7.
```

Step4: Packet data or credentials are forwarded to Verification and Validation Unit (VVU), where the biometric image separated accordingly and Sparse based Robust matching is applied to the Partial-Thumbprint, Partial-Iris and Palm-print templates in association with Biometric Database.

```
IF 'Partial-Thumprint' == 'Detected' && 'Partial-Iris' == 'Detected' && 'Palm-print' == 'Detected' GOTO Step6
ELSE Step7.
```

Step5: Packet data or credentials are forwarded to Verification and Validation Unit (VVU), where the biometric image separated accordingly and Sparse based Robust matching is applied to the Partial-Thumbprint, Partial-Iris, Partial-Palm-print and partial-face templates in association with Biometric Database.

> IF ‘Partial-Thumprint’ == ‘Detected’ && ‘Partial-Iris’ == ‘Detected’ && ‘Partial-Palm-print’ == ‘Detected’ && ‘Partial-face’ == ‘Detected’ GOTO Step6
>
> ELSE Step7.

Step6: Sent the ‘Grant’ packet of EMBSPSP to WN to access the network through Network Switch.

Step7: Sent the ‘Reject’ packet of EMBSPS to WN to check the credentials.

4. SIMULATIONS AND RESULTS

Initially Sparsed occlusion based Robust face recognition system is adopted, which was implemented in Matlab software. We tested individual and merged biometric patterns for various SL. Totally we tested 52 merged biometric samples and 38 individual patterns.The Biometric database is collected from the Biometric Research Laboratory, Swarnadhra Engg. College, IIT Delhi and IIIT Delhi [20][21][22].

4.1 Simulation of BPR at SL-3

Here the initial merged Biometric temple thumbprint is separated using partition.m file. Then the Sparse occlusion based Robust thumbprint is subjected for the detection to Thumprint-Recognition-Tool.m file and Iris also performed similarly. Figure 2 shows the partition file, Where as figure 3 shows the Robust thumbprint detection and Figure 4 shows Robust Iris detection method. The TPIR success ratio almost positive in our test with correction.

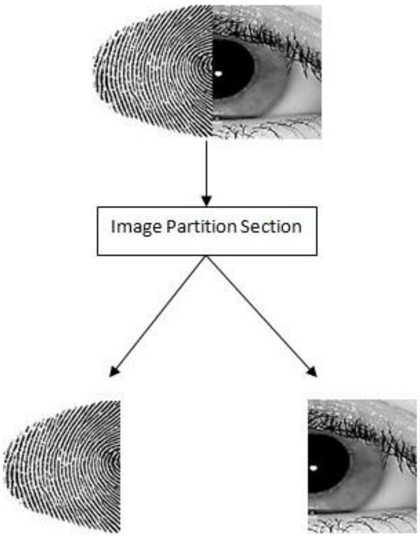


Figure 2: Partitioning the Merged-Thumprint-Iris image at SL-3

The partition has been done to all images successfully with the matlab functions.

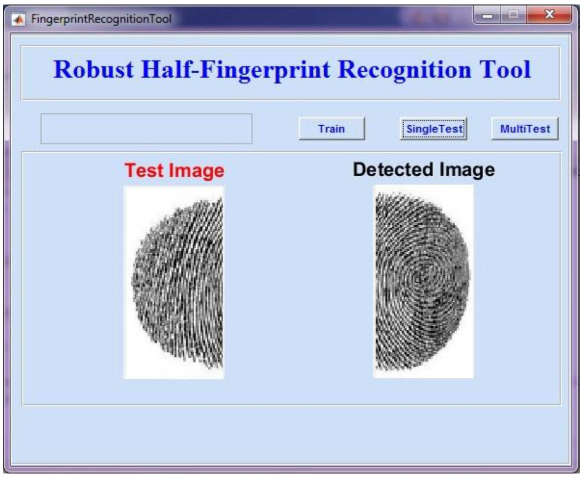

FingerprintRecognitionTool
Robust Half-Fingerprint Recognition Tool
Train
SingleTest
MultiTest
Test Image
Detected Image

Figure 3: OutputScreen of Partial fingerprint recognition at SL-3.

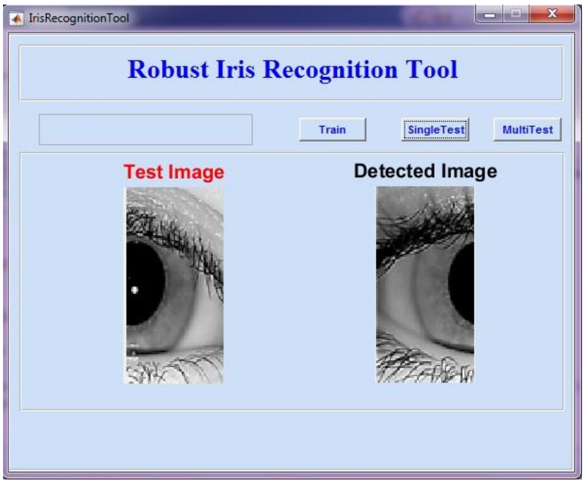
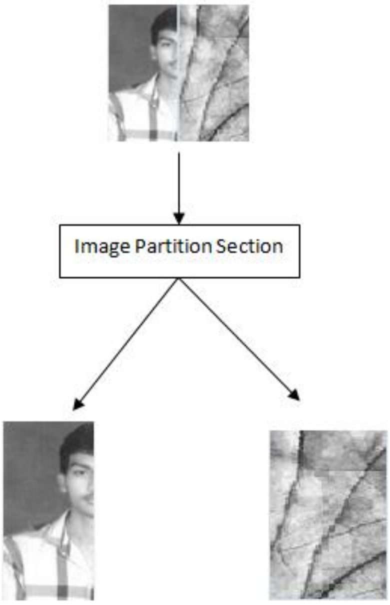


Figure 4: OutputScreen of Partial fingerprint recognition at SL-3



``

Figure 5: Partitioning the Merged-Face-Palm image at SL-5

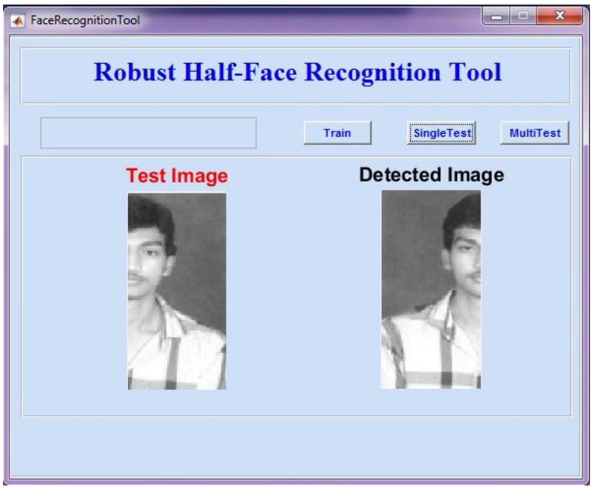


Figure 6: OutputScreen of Partial face recognition at SL-5

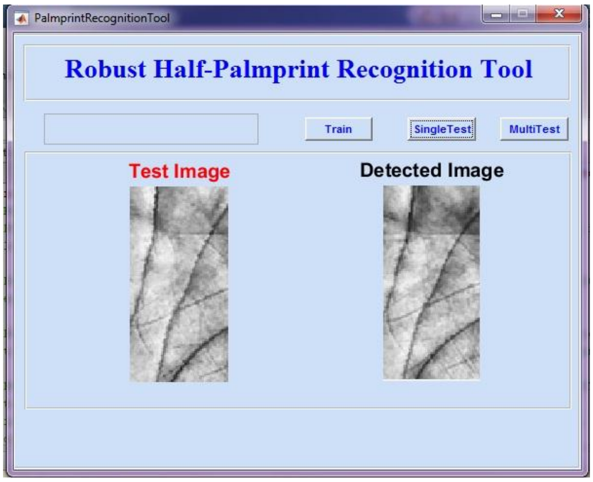


Figure 7: OutputScreen of Partial Palmprint recognition at SL-5

4.2 Overall Performance of BPA algorithm

The Overall Perfromance (OP) of BPA is impressive and the it is caliculated in equation 2.

$$OP= SL+TC+NT+TRIP-FRIP+ W^l \quad \text{-------- (2)}$$

Where SL and TC are Security level and Total computation time respectively. W^l is the pattern matching time at each SL. TRIP and FRIP are pattern matching success ratio. Lastly NT represents Network Traffic Delay.

5. CONCLUSIONS AND FUTURE SCOPE

The security is an important factor for any sort of network. Specially Wireless Network are more prone towards security threats. Beside efficiently utilizing the bandwidth through EMBSPS for the WLAN authentication. Bio-Pattern Recognitition algorithm is implemented and test successfully on the partial merged biometrics, in order to test the efficacy of the EMBSPS method authentication. Though BPR algorithm, which was built on the outcomes proves that EMBSPS approach is a better approach than earlier algorithms. But with this authentication, computation time is more, which may hamper the OP. But he BPR is best suited for occlusion based biometric pattern recognition. With BPR TIPR is almost positive, the experimental results proved it.

In future, more algorithms and more parameters are needed to be considered for better study on Bio-Pattern matching mechanism.

6. REFERENCES

[1] Akyildiz, Ian F., and Xudong Wang. "A survey on wireless mesh networks." Communications Magazine, IEEE 43.9 (2005): S23-S30.

[2] Rappaport, Theodore S. *Wireless communications: principles and practice*. Vol. 2. New Jersey: prentice hall PTR, 1996.

[3] Youssef, Moustafa A., Ashok Agrawala, and A. Udaya Shankar. "WLAN location determination via clustering and probability distributions." *Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on*. IEEE, 2003.

[4] Yao, Yu-Dong, et al. "Method/apparatus for an accelerated response to resource allocation requests in a CDMA push-to-talk system using a CDMA interconnect subsystem to route calls." U.S. Patent No. 5,983,099. 9 Nov. 1999.

[5] Andrews, Jeffrey G., Arunabha Ghosh, and Rias Muhamed. *Fundamentals of WiMAX: understanding broadband wireless networking*. Pearson Education, 2007.

[6] Sevtsuk, Andres, et al. "Mapping the MIT campus in real time using WiFi." Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City (2009).

[7] Ramesh, Avala, and S. Pallam Setty. "Enhanced Merged Security Levels of BSPS in WLAN." *International Journal of Computer Applications* 88.7 (2014): 26-34.

[8] Ramesh, Avala Ramesh and S. Pallam Setty. "Enhanced Authentication Mechanism in WLAN via MMBSPS", In IJMER, Vol-3, 4(7) , April 2014.

[9] Duvvuru, Rajesh, P. Jagadeeswara Rao, and Sunil Kumar Singh. "Improvizing Security levels in WLAN via Novel BSPS." Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013 International Conference on. IEEE, 2013.

[10] Wright, John, et al. "Robust face recognition via sparse representation." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 31.2 (2009): 210-227.

[11] Jea, Tsai-Yang, and Venu Govindaraju. "A minutia-based partial fingerprint recognition system." *Pattern Recognition* 38.10 (2005): 1672-1684.

[12] Zhang, Dapeng, and Wei Shu. "Two novel characteristics in palmprint verification: datum point invariance and line feature matching." *Pattern Recognition* 32.4 (1999): 691-702.

[13] Pillai, Jaishanker K., et al. "Secure and robust iris recognition using random projections and sparse representations." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 33.9 (2011): 1877-1893.

[14] Duvvuru, Rajesh, et al. "Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via

ARSA." *Quality, Reliability, Security and Robustness in Heterogeneous Networks*. Springer Berlin Heidelberg, 2013. 185-196.

[15] Duvvuru, Rajesh, P. Jagadeeswara Rao, Sunil Kumar Singh, and Ankita Sinha. "Enhanced Security levels of BSPS in WLAN." *International Journal of Computer Applications* 84, no. 2 (2013): 33-39.

[16] Kumar, Sanjay. "Enhancing the Security Levels in WLAN via Novel IBSPS." *Advanced Computing, Networking and Informatics-Volume 2*. Springer International Publishing, 2014. 351-359.

[17] Ramesh, Avala, and S. Pallam Setty. "A Comparative Study on Security Levels in WLAN." *International Journal of Computer Applications* 93.8 (2014): 11-17.

[18] Godi, Sudhakar. "Improved Security Levels of Wireless LAN through DBSPS." *International Journal of Computer Applications* 106, no. 14 (2014).

[19] Geddada, Uma Devi, and Kaligithi Rajesh Kumar. "MMBWPS FOR STRENGTHENING AUTHENTICATION PROCESS IN WIRELESS LOCAL AREA NETWORKS." Published in International Jounral of Computer applications and Engineering,, vol-8, 1(1), 174-184.

[20] Ajay Kumar, "Incorporating Cohort Information for Reliable Palmprint Authentication," Proc. ICVGIP, Bhubneshwar, India, pp. 583-590, Dec. 2008

[21] Ajay Kumar, Sumit Shekhar, "Personal Identification using Rank-level Fusion," IEEE Trans. Systems, Man, and Cybernetics: Part C, pp. 743-752, vol. 41, no. 5, Sep. 2011.

[22] D. Yadav, N. Kohli, R. Singh, and M. Vatsa, Revisiting Iris Recognition with Color CosmeticContact Lenses, 6th IAPR International Conference on Biometrics, June, 2013.