International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

A Secure Boot Loader System for Loading an Operating System with Fingerprint Authentication

Alycia Sebastian, K.Siva Sankar

Abstract— In today's world, people are constantly on move and portable systems are in demand. With technology advancement, people exploit different types of memory devices for a portable system. For any external boot medium, the BIOS boot order setting change is required. The dynamic boot loader successfully eliminated this dependency and allowed the user to directly boot from any portable USB. The usage of USB has grown exponentially in recent years and securing it has become a major concern. In this paper, the USB is devised as a highly secured portable boot medium with fingerprint authentication to ensure data security. It performs feature extraction by combining both Local Directional Pattern (LDP) and Histograms of Oriented Gradients (HOG) which improves the accuracy rate. The classification is performed by random forest classifier, such that the intended users alone are granted access to the private storage area of the USB drive.

Index Terms—Flash Memories, Fingerprint Recognition, Operating Systems, Portable computers

I. INTRODUCTION

Owing to the small but powerful nature of Universal Serial Bus (USB) flash drives are widely utilized by today's technological community [1]. The USB devices are meant for data storage and can be plugged in or removed, whenever necessary. The major advantages of USB flash drives are its size, portability and reusability. USB flash drives come into picture in 2000s and the greatest possible storage capacity supported by USB drives is 2 TeraBytes (TB), as on 2018 [2]. Additionally, the USB drives withstand electromagnetic interference and exterior scratches. Recognizing these advantages, most of the users exploit these USB drives. A standard USB drive consists of five significant parts and they are USB plug, storage controller, memory chip, crystal oscillator and a cover. The USB plug enables the device to get plugged in the computer and the storage controller is based on a microcontroller with on-chip Random Access Memory (RAM) and Read Only Memory (ROM). The memory chip is meant for data storage and the crystal oscillator manages the outcome of the device with the help of a phase-locked loop. Finally, a cover is included to wrap all the internal components of the device.

Though USB is a portable and convenient device, it is susceptible to several security threats. In most of the cases, the USB attacks are triggered on the storage [3]. In order to deal with this, several Operating Systems (OS) intend to restrict the access grants to the system resources and the autorun feature of the USB is debilitated. However, the USB devices are easily prone to security attacks, which results in serious data loss or damage. Biometric ased security is considered as reliable and robust, as the biological characteristics of humans of distinct and constant. Hence, USB manufacturers provide security to the USB drive through software and hardware based protection schemes. USB device with in-built fingerprint scanner and password protection are freely available in the market. Regular USB drives can also be integrated with the fingerprint scanner to implement fingerprint security in the system. Considering this point, this work attempts to improvise the previously proposed work, which presents a dynamic boot loader for loading an OS [4, 5] by providing the biometric authentication to secure the Live USB. The dynamic boot loader program simplifies the process to boot from external medium without changing the boot order settings. The fingerprint authentication system relies on three key phases and they are fingerprint pre-processing, feature extraction and recognition phases. The outcome of each phase is passed as an input to the forthcoming phase. The performance of the proposed approach is then analysed in terms of standard performance metrics. The rest of the article is organised as follows. Section 2 reviews the related literature with respect to USB and fingerprint authentication scheme. Section 3 presents the proposed authentication system for the boot loader and the performance of the proposed approach is evaluated in section 4. Section 5 concludes the article.

II. REVIEW OF LITERATURE

Several research works have been successfully presented in the existing literature for safeguarding the USB information from unauthorized access, however setting a safe environment is more important in providing data protection. In [6], the authors have discussed bootable USB as the alternative for CD/ DVD. The paper discusses to boot multiple OS from ISO images by utilizing USB disk. Many researchers have explored the usage of USB as a portable medium and analyzed its security vulnerabilities.

Manuscript published on 30 August 2019.
*****Correspondence Author(s)
Alycia Sebastian*, Research Scholar, Department of Computer Science & Engineering, Noorul Islam Centre for Higher Education, Thuckalay, TamilNadu, India,alycia.sebastian@gmail.com
Dr. Siva Sankar, Associate Professor, Department of Information Technology, Noorul Islam Centre for Higher Education, Thuckalay, TamilNadu, India, sivasankarniu@gmail.com

The Universal Serial Bus (USB) is a mass storage device, which is vulnerable to attacks. In [7], the authors have proposed a control algorithm for mutual authentication between the server and USB to protect USB documents. The user has to authenticate the identity with user name and password. A session key is then generated based on the username and ID of the USB device. The generated key is used to encrypt the files being stored in the USB device. The server stores the client session key temporarily which poses serious threat to the USB data. In [8], the authors have discussed the security threats of various protocol used for securing USB flash drive. The authors have proposed software based secure USB mechanism where the registration and authentication program runs in the host machine which limits the concept of portability. Biometric authentication gives the user the advantage of using USB as a portable system on any host machine. USB is the most popular portable storage device. Once it is lost, the information in the USB is prone to theft. In [9], the authors have discussed various ways of securing USB memories, while analyzing its vulnerabilities. The approaches to secure USB can be categorized under software only approach, hardware supported partitioning approach and Hardware based encryption approach [10]. The authors discussed different types of authentication protocol and its vulnerabilities and concluded that it is more secure to perform authentication in the removable device itself. Biometric authentication has become popular, because of successful attacks on password and PIN's. In USB token fingerprint authentication system, the patterns are stored in USB token but, preprocessing is done in the computer system that makes the entire authentication system vulnerable to attack. This disadvantage can be overcome by performing fingerprint matching inside the USB token system [11]. In [12], the authors successfully bypassed the fingerprint authentication by making binary code modification in .dll file. A program is developed to retrieve the fingerprint reference templates from the drive, which poses serious security threat to user data in the USB. The security analysis was based on drive which uses the host system for fingerprint enrollment and verification. In [13], the feature extraction is performed by combining HOG and LBP and classification is done by comparing SVM and Random Forest classifier. The analysis found random classifier with more accuracy rate. The feature extracted is larger in dimension and time consumption is relatively more. The paper [14] performs study on feature extraction by LBP and LDP and observed that LBP has better performance than LDP but has higher dimensions. The USB with its high storage capacity, low cost, low power consumption and portability, the usage of USB is increasing rapidly. Many researchers has identified USB as a better portable medium and proposed method for securing the USB. Motivated by the existing approaches, the proposed approach intends to present fingerprint authentication based security for USB device and the proposed work is elaborated in the following section.

III. PROPOSED FINGERPRINT AUTHENTICATION SYSTEM BASED SECURITY FOR USB

This section describes the booting process and the architecture of the USB, followed by which the fingerprint authentication system is presented. There are different approaches to secure USB device from unauthorized access. The security on stored data becomes meaningless, when secure USB is used with a hostile host system. The attackers can bypass the fingerprint authentication system and access the stored data. To eliminate this type of attack, the paper proposes a plug and play Live USB, where the fingerprint authentication is done before the OS is loaded from USB to RAM. The authentication scheme along with the OS runs from the USB and is independent of the hostile system. This method guarantees a safe, secure and reliable portable system for user data. Hence, the user can store highly confidential information on live USB and can be used in any host system that supports USB booting. Whenever the user plugs in the USB to any system, a window pops up to know whether the user needs to boot from USB. In case of this requirement, the system prompts the user to verify the access rights. Once authorized, the private partition of USB opens and the dynamic boot loader application starts running, which loads OS from USB. This idea improves the user experience and conserves memory as well. The following section discusses about the standard architecture of USB.

IV. PROPOSED USB ARCHITECTURE

A 16 GB USB is used in which the storage space is divided into 2 partitions and they are private and public. The architecture of USB is shown in figure 2.

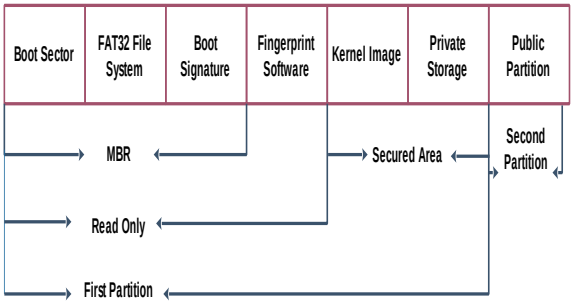

Figure1. Proposed USB architecture

The dynamic boot loader and fingerprint application are read by BIOS to detect the USB at boot time. The first partition of the USB contains the Master Boot Record (MBR) that has the boot loader, FAT32 file system, partition table and Disk signature [10]. The FAT32 file system is used, so that the USB can be used in almost all system that supports USB. The USB is hardware encrypted. The OS and the private sectors are protected with the help of user fingerprint. When the USB device is plugged in, the read only files and public storage are visible. The private partition is granted access to the user upon the successful completion of the user identity with the help of fingerprint and the authorized user can reboot the system from USB. The second partition is the public partition, which is available for normal data storage. The user can use the USB as normal data storage medium as well. Hence, the concept of security is incorporated to the proposed approach by employing fingerprint authentication and the processes involved in fingerprint authentication are presented in the following section.

Retrieval Number: E7649068519/19©BEIESP
DOI: 10.35940/ijitee.B7649.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

V. PROPOSED FINGERPRINT SYSTEM

Fingerprint is one of the powerful biometrics that can discriminate between the individuals effectively. The fingerprints can be captured on the go without any special requirements. Hence, this biometric is chosen to ascertain the security of the proposed approach. Whenever the user needs to access the private storage space of the USB drive, the user needs to pass through this security line. This idea helps in controlling the unintended accesses and alterations on the USB. Hence, the system employs a separate module for processing the fingerprints of the user. The block diagram for the proposed fingerprint system is shown in figure 2.

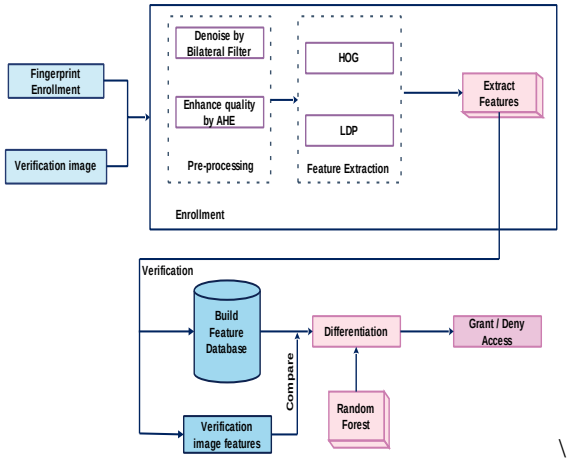

Figure 2. Block Diagram for proposed Fingerprint System

This module recognizes the fingerprint of various users and the access is provided to the user upon perfect match. The process of fingerprint recognition is based on three significant phases and they are fingerprint image pre-processing, feature extraction and recognition. The image pre-processing phase aims to prepare the images suitable for the forthcoming processes. This phase may involve in denoising, quality enhancement and so on. This work attempts to denoise and enhance the fingerprint images by means of bilateral filter and adaptive histogram equalization techniques respectively. The so pre-processed images are then treated by the feature extraction phase, which extracts the Local Directional Pattern (LDP) and Histograms of Oriented Gradients (HOG). The feature vectors are formed during the enrolment stage and the fingerprint is recognized in the verification phase by matching the captured fingerprint with the database. This process of matching is performed by random forest classifier.

A. Fingerprint image pre-processing

As soon as the fingerprint images are captured, the images are pre-processed to remove redundant or unwanted information that may occur during image acquisition. In this work, the image pre-processing phase performs two basic functionalities such as image denoising and quality enhancement. The denoising procedure removes noisy information from the image and the quality is enhanced for discriminating the areas in the images. The better the pre-processing activity, the better is the recognition performance. Some of the sample pre-processed images are shown in figure 3.

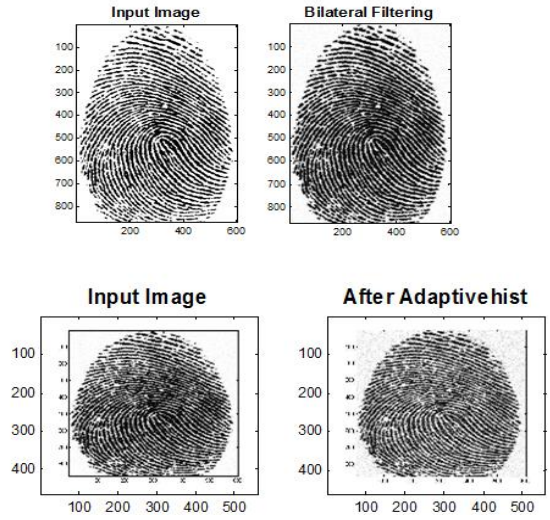

Figure.3. Images after Bilateral Filter and Apative Histogram Equalization

This work denoises the fingerprint images with the help of bilateral filter and the image quality enhancement is achieved by adaptive histogram equalization technique. Bilateral filter considers the total weights of the pixels in a specific local neighbourhood window and the pixel weights are calculated by the distance of spatial and intensity value distribution [15]. This work nature of bilateral filter preserves the edge information of the images and the noise in the images is removed by computing the mean value as represented in equation 1.

$$BF(pix_i) = \frac{1}{c}\sum_{pix_j \in NH(pix_i)} e^{\frac{-\left\|pix_j - pix_i\right\|^2}{2\sigma_{sd}^2}} e^{\frac{-|In(pix_j) - In(pix_i)|^2}{2\sigma_{sr}^2}} In(pix_j) \quad (1)$$

where σ_{sd} and σ_{sr} are the control parameters with respect to the spatial and intensity domains. $NH(pix_i)$ indicates the spatial neighbourhood of pixel $BF(pix_i)$ and c is the constant denoted by

$$c = \sum_{pix_j \in NH(pix_i)} e^{\frac{-\left\|pix_j - pix_i\right\|^2}{2\sigma_{sd}^2}} e^{\frac{-|In(pix_j) - In(pix_i)|^2}{2\sigma_{sr}^2}} \quad (2)$$

These denoised fingerprint images are then treated by adaptive histogram equalization technique, which processes the pixels with respect to adaptive window size [16]. By this operation, the contrast levels of the pixels are improved and finally all the contrast enhanced windows are clubbed together by bilinear interpolation operation to discard temporary edges. Hence, the fingerprint images are pre-processed and are suitable for feature extraction phase, as presented below.

B. HOG and LDP Feature Extraction

The pre-processed images are passed as input to the feature extraction phase, which is based on HOG [17] and LDP [18]. HOG features are so popular in determining the look and shape of the image, however utilization of HOG features alone cannot achieve better recognition accuracy.

When the HOG features are accompanied with the LDP features, the performance of the recognition goes better. The LDP features rely on the image gradients, which are more consistent than the image intensity. Hence, this work extracts both these features to form the feature vector.

The HOG feature is computed by taking both the gradient magnitude and direction of the image into account. Initially, decompose the complete fingerprint image into $n \times n$ cells without any overlap and pixel blocks are created by clubbing $bl_1 \times bl_2$ blocks. For a specific pixel, the gradient is computed both in horizontal and vertical directions by means of a single dimensional mask template [-1 0 1], as represented by equation 3.

$$GA_x(a,b) = I(a+1,b) - I(a-1,b) \quad (3)$$

$$GA_y(a,b) = I(a,b+1) - I(a,b-1) \quad (4)$$

In the above equations, $GA_x(a,b)$ and $GA_y(a,b)$ represent the amplitudes of horizontal and vertical gradients respectively. The $I(a,b)$ represents the corresponding value of the pixel (a,b). The gradient magnitude and orientation are computed by the following equations.

$$mg(a,b) = \sqrt{GAx^2 + GAy^2} \quad (5)$$

$$\theta(a,b) = \tan^{-1}\left(\frac{GA_x}{GA_y}\right) \quad (6)$$

This range of orientation starting from 0° to 180° is separated into r bins for computing the histogram of every cell as in equation (7).

$$HC(r)_i = HC(r)_i + mg(a,b) \quad (7)$$

The histograms of blocks are then computed by combining the HCs together, as given by the following equation.

$$HB_k = \{HC_1, HC_2, \dots, HC_{bl_1 \times bl_2}\} \quad (8)$$

This vector is then normalized by means of L2 normalization as follows.

$$N(HB_k) = \frac{HB_r}{\sqrt{||HB||_2^2 + e^2}} \quad (9)$$

In the above equation, e is a constant and the total count of bins is fixed as 9. The final HOG is returned by

$$HOG = \{N(HB_1), N(HB_2), \dots, N(HB_k) \dots, N(HB_N) \quad (10)$$

Hence, the HOG features are extracted from the image and the LDP features are computed as follows.

As stated earlier, the LDP is chosen because of its consistency, as it is based on gradients. LDP manipulates the images in different directions and every pixel is denoted by an eight bit binary code. For example, let Img be an image with pixels (a_i, b_i). The Kirsch compass edge detector is employed to detect eight directional outcomes (dr_o) as indicated by the following equation.

$$dr_{o_i} = \sum_{p=-1}^{1}\sum_{q=-1}^{1} Ms_{dr}(p+1, q+1) \times Img(a+p, b+q) \quad (11)$$

The $dr_{o_i}\ (i = 1,2,\dots,7)$ is computed for all the eight directions and all the eight directional outputs are indicated by codes. This code allots the value 1 to a particular bit and the remaining bits are set to 0. This assignment is performed for s number of directional outputs and the processed bit is fixed as 1 and $8-k$ bits are assigned as 0. Finally, the overall directional outcomes of a pixel are denoted by

$$LDP_{a,b}(op_1, op_2, \dots, op_8) = \sum_{i=1}^{8} t(op_i - op_k) \times 2^i \quad (12)$$

$$t(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \quad (13)$$

where op_k is the k^{th} significant directional outcome. Here, the value of k is increased from the value of 1 to 5 and better results are attained when k is 3. By this way, the LDP codes are formed for all the image pixels and the LDP histogram is built.

$$LDP_{his} = \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} P(LDP_{(a,b)}, LDP_{p_i}) \quad (14)$$

LDP_{p_i} is the i^{th} pattern value of LDP and it differs with the value of k. P is fixed as 1 when the value of x is 0 and 0 otherwise. Hence, the LDP features are extracted and the features are clubbed together.

$$fv_i = \{HOG \cup LDP_{his}\}_i \quad (15)$$

As the HOG and LDP features are clubbed together, the feature set is voluminous and the features are needed to be reduced with the help of Information Gain Ratio (IGR).

C. Feature Dimensionality Reduction by IGR

This work minimizes the dimensionality of the feature set by employing IGR, which is an enhanced version of information gain [19]. The IGR takes the distinct values into account and is computed by

$$IGR(ftr) = \left(\frac{IG_{fts} - IG_{ftr}}{IG_{fts} + IG_{ftr}}\right) \times 100 \quad (16)$$

Where IG_{fts} and IG_{ft} are represented as follows.

$$IG_{fts} = -\left[\frac{rf(c_1, fts}{|fts|}\right] \log_2 \left[\frac{rf(c_1, fts}{|fts|}\right] \quad (17)$$

$$IG_{ftr} = \left[\frac{|ftr_i|}{|ftr|}\right] \times IG_{ftr_i} \quad (18)$$

Retrieval Number: E7649068519/19©BEIESP
DOI: 10.35940/ijitee.B7649.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The term $\left[\frac{rf(c_1,fts}{|fts|}\right]$ indicates the frequency of a specific feature, which is present in class c_1. Consider a feature ftr which has l different values represented by $\{ftr_1, ftr_2, \dots, ftr_l\}$, with l different subclasses such as $\{c_1, c_2, \dots, c_l\}$. Thus, the $IGR(ftr)$ is calculated for all the features and the features with maximum IGR are taken into account. This kind of feature dimensionality minimization paves way for memory and time conservation. The optimal features alone are considered by the classifier to recognise the fingerprint. This work employs random forest classifier for recognizing the users.

D. User Recognition by Random Forest Classifier

The legitimate and the illegitimate users are differentiated by means of random forest classifier. Consider R be the total number of random trees in the forest and the enrolled set is denoted as ES. During the process of enrolment, each tree is allotted with the weight of $W_i^0 = 1$; where $i = \{1, Q\}$. The probability of class label cl for image β is denoted by $p_i^{cl}(\beta)$ and is determined by the tree i. The weight of the tree is computed by

$$W_i = W_i^0 - \frac{1}{ES}\sum_{k=1}^{ES}\left|p_i^{\bar{cl}}(k) - p_i^{cl}(k)\right|; i = \{1, Q\} \quad (19)$$

In equation (19), $p_i^{\bar{cl}}(k)$ denotes the label of ground truth sample. In the verification phase, the recognition is carried as follows. Let b be the total count of classes for the input data k, then the classification is performed by the following equation.

$$\bar{cl} = \underset{c}{argmax} \sum_{i=1}^{T} W_i\, p_i^{cl}(k); i = \{1, Q\} \quad (20)$$

This random forest based classification provides better recognition results [20], as the weight assignment and the trees with minimal weights cannot achieve better results. The performance of the proposed approach is evaluated and the experimental results are presented in the following section.

VI. RESULTS AND DISCUSSION

This section intends to justify the performance of the proposed approach by checking the false acceptance rate, false rejection rate, accurate recognition rates and time consumption analysis. In order to evaluate the proposed approach, this work enrols 100 fingerprints from twenty five persons. The features of the fingerprints are extracted to form the feature vector and the feature vectors are stored in the database. In the verification phase, the fingerprint image is captured from the user and the HOG, LDP features are extracted from the fingerprint images. The feature vector is formed and the random forest classifier is employed to distinguish between the users. When the user successfully passes the authentication process, the user is given access to the private storage space of the USB drive. Hence, the authentication system must work with better accuracy, such that the unintended users are denied access, while intended users are granted users. This is possible only with minimal false acceptance and false rejection rates. Both these measures are computed by the following equations.

$$FAR = \frac{Total\ count\ of\ access\ grants\ to\ unintended\ users}{Total\ access\ grants\ and\ denials} \quad (21)$$

$$FRR = \frac{Total\ count\ of\ access\ denials\ to\ intended\ users}{Total\ access\ grants\ and\ denials} \quad (22)$$

The performance of the proposed approach is compared in three ways such as by varying the feature extraction and classification techniques. Additionally, the potential of feature dimensionality reduction is proven by including and excluding the IGR. The fingerprint recognition system is evaluated by utilizing HOG, LDP and the combination of HOG and LDP features. The performances of the features are evaluated and the results are presented in the following figures.

Performance comparison by varying the feature extraction techniques

Feature extraction is the vital part of any classification based application. The classifier performs better, when the potential features are extracted from the images. The combination of HoG and LDP proves better performance than when utilized individually. This statement is proven by the following results depicted in figure 4 and 5.

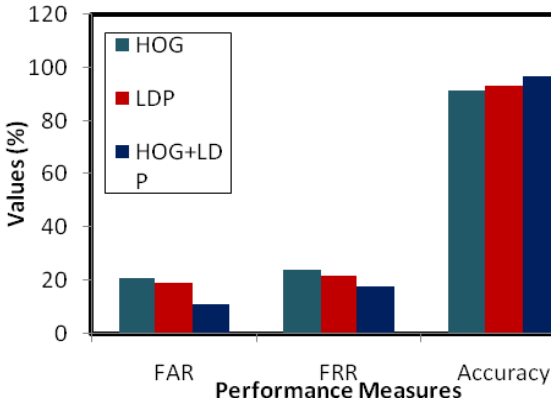

Figure.4. Comparative results w.r.t feature extractors

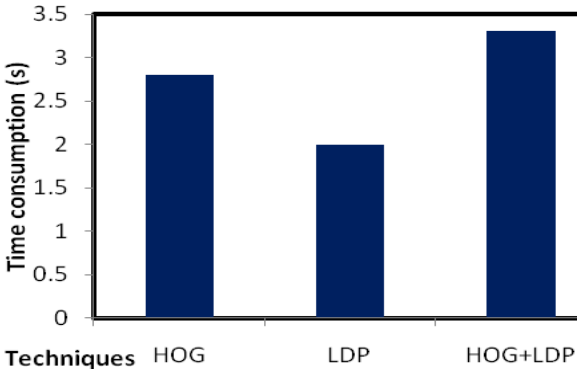

Figure 5. Time consumption analysis

From the experimental results, it is proven that the combination of HOG and LDP features perform better with respect to false acceptance and false rejection rates. The greater false acceptance rates mean that the system grants access to the private storage space of the USB to the illegitimate or the malicious users. Similarly, more false rejection rates indicate that the legitimate users are denied access to the private storage space of the USB. Both these issues are equally serious and the lesser the false acceptance and false rejection rates, the better is the efficiency of the system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

On experimental analysis, the results prove that the proposed work involves minimal false acceptance and false rejection rates, which in turn enhances the accuracy rates of the system. As far as time consumption is concerned, the proposed approach consumes time with minimal difference when compared to the feature extractors. The time consumption is measured in seconds. The time consumption analysis is carried out on a stand alone system with 8 GB RAM and the performance of the proposed approach is satisfactory.

A. Performance comparison by varying the classification techniques

The classifiers are the final decision makers to distinguish between the legitimate and illegitimate users. The choice of random forest classifier is justified by comparing the performance with the popular classifiers such as k-Nearest Neighbour (k-NN) [21] and Relevance Vector Machine (RVM) [22]. The main reason for the choice of random forest classifier is its simplicity and greater accuracy rates. The performance of the classifiers is tested with the combination of HoG and LDP features. The results attained by the comparative classifiers are presented as follows.

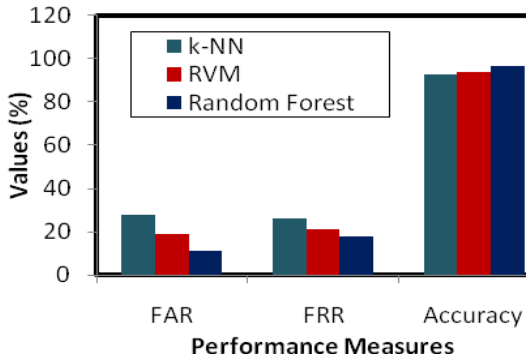

Figure.6. Performance comparison by varying classifiers

On analysing time consumption of the classifiers with the combination of HoG and LDP features, random forest performs better rather than k-NN and RVM classifiers. As random forest is capable of attaining better results with the better learning capability, the performance of random forest is better than the k-NN and RVM. k-NN consumes more time for result declaration, as there is a need to determine the value of k and to perform comparison between the entities. Similarly, RVM suffers from computational and time complexity, such that it consumes more time for returning the result. The time consumption analysis of the proposed work is as follows.

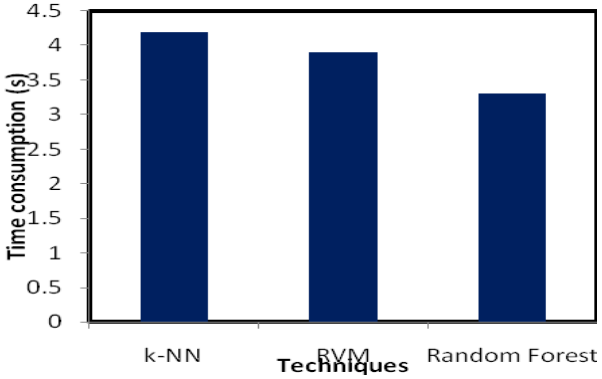

Figure 7. Time consumption analysis by varying the classifiers

Hence, the potential of random forest classifier is proven and the following graph lays stress on the potential of the feature dimensionality reduction by IGR. The main objective of including IGR is to reduce the time consumption of carrying out the proposed work and the following graph shows the results attained with and without IGR.

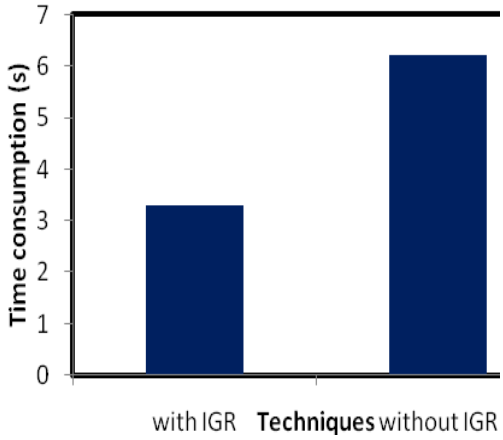

Figure 8. Time consumption analysis with and without IGR

When the IGR is not included for feature dimensionality reduction, then the proposed work suffers from more time consumption, which degrades the performance. The time consumption is almost double without IGR. Hence in order to improve the performance, the proposed work employs IGR for reduced time consumption and computational complexity. Hence, the objective of the proposed work is attained in a reasonable period of time and the following section concludes the article.

VII. CONCLUSION

The proposed USB devised as a bootable medium with integrated fingerprint authentication provides a highly portable and secure USB system, which can guarantee confidentiality for the information stored on the USB. Since the OS can be customized as per the need of the user, the loading time is much reduced. Integrating the concept of dynamic boot loader which automatically identifies the Live USB [4], with fingerprint will provide a user friendly environment to the user. Both data security and user friendly environment is offered to the user. All the fingerprint operation is done inside the USB without involving the host system. This eliminates the need to transfer fingerprint images between host and USB, thus securing the pattern. The USB can be used in any machine irrespective of the OS installed in that system. In future, the fingerprint can be accompanied by some other biometric to boost up the security.

REFERENCES

1. Tetmeyer, A., & Saiedian, H, “Security threats and mitigating risk for USB devices”, IEEE Technology and Society Magazine, 29(4), p.44-49, 2010.
2. https://www.digitaltrends.com/computing/largest-flash-drives/

Retrieval Number: E7649068519/19©BEIESP
DOI: 10.35940/ijitee.B7649.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

3. Pham, D. V., Syed, A., & Halgamuge, M. N, "Universal serial bus based software attacks and protection solutions", Digital investigation, 7(3), 172-184, 2011.
4. Alycia Sebastian, Dr. K. Siva Sankar," Design of a Dynamic Boot Loader for loading an Operating System", Journal of Computer Science, volume 15, no.1, p.190-196, 2019.
5. Alycia Sebastian, Dr. K. Siva Sankar," Design of a Boot Loader for Operating System", Australian Journal of Basic and Applied Sciences, volume 9, no 2, p. 368-374, 2015.
6. Sivaiah, B., Murthy, T. S. N., & Babu, T. V, "Boot multiple Operating Systems from ISO images using USB Disk", IEEE International Conference on Electronics and Communication Systems (ICECS), p. 1-5, February 2014.Daesung Moon, Youn hee Gil, Dosung Ahn, Sung Bum Pan, [7] Mr. A. N. Magdum, Dr. Y. M. Patil," A Secure Data Transfer Algorithm for USB Mass Storage Devices to Protect Documents", International Journal of Emerging Engineering Research and Technology, volume 2, no 4, p.78-84, July 2014.
7. Kyungroul Lee, Insu Oh, Yeunsu Lee, Hyeji Lee, Kangbin Yim, and Jungtaek Seo, "A Study on a Secure USB Mechanism That Prevents the Exposure of Authentication Information for Smart Human Care Services," Journal of Sensors, volume 2018(1) , p.1- 17, 2018.
8. Kyungroul Lee, Hyeungjun Yeuk, Youngtae Choi, Sitha Pho, Ilsun You, Kangbin Yim, "Safe Authentication Protocol for Secure USB Memories", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume 1, no. 1, p. 46-55, 2010.
9. Jaein Kim, Youngjun Lee, Kyungroul Lee, Taeyoung Jung, Dmitry Volokhov, and Kangbin Yim, " Vulnerability to Flash Controller for Secure USB Drives", Journal of Internet Services and Information Security (JISIS), volume 3, no. 3/4, p. 136-145, November 2013.
10. Yongwha Chung and Chee Hamg Park. "Fingerprint Based Authentication for USB Token Systems", Information security Applications, Volume 2908 of the series Lecture Notes in Computer Science, p. 355-364, 2004.
11. Benjamin Rodes, Xunhua Wang, "Security analysis of a fingerprint-protected USB drive", Proceedings of the 26th Annual Computer Security Applications Conference, p. 89-96, December 2010.
12. Jeena Sara Viju, Sruthy, "SVM and Random Forest Classification Methods for Fingerprint Liveness Detection", International Research Journal of Engineering and Technology, volume 5, no.2, February 2018.
13. Bo Xu, Daozhi Lin, Lonbiao Wang, Hongyang Chao, Weifeng Li and Qinmin Liao, "Performance comparison of local directional pattern to local binary pattern in off-line signature verification system", IEEE 7th International Congress on Image and Signal Processing, January 2015.
14. Tomasi, C., & Manduchi, R, "Bilateral filtering for gray and color images", Proceedings of the 1998 IEEE International Conference on Computer Vision, p. 839), January 1998.
15. Stark, J. A, "Adaptive image contrast enhancement using generalizations of histogram equalization", IEEE Transactions on image processing, volume 9, no.5, p. 889-896, 2000
16. Dalal, N., & Triggs, B, "Histograms of oriented gradients for human detection", International Conference on computer vision & Pattern Recognition (CVPR'05) IEEE Computer Society, volume 1, p. 886-893), June 2005.
17. Jabid, T., Kabir, M. H., & Chae, O, "Local directional pattern (LDP)–A robust image descriptor for object recognition",7th IEEE International Conference on Advanced Video and Signal Based Surveillance, p.482-487, August 2010.
18. Mori, T, "Information gain ratio as term weight: the case of summarization of IR results Proceedings of the 19th international conference on Computational linguistics, volume 1, p.1-7, September 2002.
19. Denil, M., Matheson, D., & De Freitas, N, "Narrowing the gap: Random forests in theory and in practice", International conference on machine learning, p. 665-673, January 2014.
20. Cunningham, P., & Delany, S. J, "k-Nearest neighbour classifiers", Multiple Classifier Systems, volume 34, no. 8, p. 1-17, 2007.
21. Tipping, M. E, "The relevance vector machine", In Advances in neural information processing systems, p. 652-658 , 2007.

Author profile

Ms. Alycia Sebastian is pursuing PhD in the field of Operating System. She is currently working as Assistant Professor in Waljat College of Applied Sciences, Muscat, Sultanate of Oman from 2009 to till date. She has more than 11 years experience in teaching field. She is an active member of Oman Society of Engineers (OSE). Her area of interest is Operating system, System software and Compiler Design.

Co-Author

Dr. Siva Sankar Kanahasabapathy received his doctorate degree from MS University, TamilNadu, India. He is currently working as Associate Professor from 2009 in Noorul Islam Centre for Higher Education, TamilNadu, India. He is well known for his research in the field of System Software and Embedded systems and has published more than 26 articles in International Journal and Conferences. He is also reviewer of various reputed International Journals.