Electronic Commerce Research and Applications 18 (2016) 71–82

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

Face recognition using support vector model classifier for user authentication

Wen-Hui Lin [a,*], Ping Wang [a], Chen-Fang Tsai [b]

[a] Department of Information Management, Kun Shan University, Tainan, Taiwan
[b] Department of Industrial Engineering Management, Aletheia University, Tanshui, Taiwan

ARTICLE INFO

Article history:
Received 12 March 2015
Received in revised form 24 January 2016
Accepted 31 January 2016
Available online 9 February 2016

Keywords:
E-commerce
SVM
Face recognition
Wavelet transforms
Local binary pattern

ABSTRACT

Most existing user authentication approaches for detecting fraud in e-commerce applications have focused on Secure Sockets Layer (SSL)-based authentication to inspect a username and a password from a server, rather than the inspection of personal biometric information. Because of the lack of support for mutual authentication or two-way authentication between a consumer and a mercantile agent, one-way SSL authentication cannot prevent man-in-the-middle attacks. In practice, in user authentication systems, machine learning and the generalisation capability of support vector models (SVMs) are used to guarantee a small classification error. This study developed an online face-recognition system by training an SVM classifier based on user facial features associated with wavelet transforms and a spatially enhanced local binary pattern. A cross-validation scheme and SVMs associated with the Olivetti Research Laboratory database of user facial features were used for solving classification precision problems. Experimental results showed that the classification error decreased with an increase in the size of the training samples. By using the aggregation of both the low-resolution and the high-resolution face image samples, the global precision of face recognition was over 97% with tenfold cross-validation scheme for an image data size of 168 and 341, respectively. Overall, the proposed scheme provided a higher precision of face recognition compared with the average precision for low-resolution face image (approximately 89%) of the existing schemes.

1. Introduction

E-commerce applications have been increasing rapidly. Service providers are expected to guarantee secure transaction authentication for Web services. While Web services provide e-commerce applications that offer valuable opportunities, Web services face major challenges since consumers are reluctant to avail e-commerce services in the absence of service provider guarantees regarding the security of their information. In particular, Secure Sockets Layer (SSL)-based authentication provides an efficient and economical means of using the standard username/password convention. However, one-way SSL authentication cannot prevent cyber attacks such as phishing and man-in-the-middle attacks, which is a major obstacle to consumer adoption of e-commerce. Generally, when using a banking mobile app to access banking services online, people never think that they could become a victim of identity theft. According to reports released by privacy IT Security in the United States, hackers had gained root access to 90 servers of a financial institution's servers in 2014, and the access enabled the hackers to transfer funds, disclose customer information, open new accounts, and even close accounts without prior knowledge of the affected customers (IT Security 2015). Because of the nondenial requirements of remote user identity authentication schemes, such access is most commonly achieved using a biometrics-based approach.

Identity theft is therefore one of the most severe threats to the security of online transactions associated with e-commerce services. Consequently, it is imperative that service providers have the means to authenticate the identity of every user for detecting fraud. Efficient user authentication schemes are required to build trust in e-commerce, and mutual authentication schemes are crucial for e-commerce applications. As the sophistication of tools used by malicious users continues to increase, the data processed in e-commerce are at increased risk of attack. Consequently, there is an urgent need for robust authentication schemes that can confine data access to legitimate, authorised users by preventing malware from tracking transactions during authenticated sessions.

* Corresponding author.
E-mail addresses: linwh@mail.ksu.edu.tw (W.-H. Lin), pingwang@mail.ksu.edu.tw (P. Wang), au1204@mail.au.edu.tw (C.-F. Tsai).

http://dx.doi.org/10.1016/j.elerap.2016.01.005
1567-4223/

Multifactor authentication approaches in which digital certificates are provided to users by a public key infrastructure mechanism have been developed for user authentication systems. These approaches enable detecting fraudulent use of user identity because they involve using face-recognition information, radio frequency identification (RFID) tags, and machine learning (ML) techniques. Numerous two-factor improvement methods (Min et al. 2011, Jing et al. 2009, Nguyen et al. 2012, Yang et al. 2012, Battaglia et al. 2014) have been proposed. Authors incorporated a face-recognition feature into a smart card, and images of each user with different facial expressions were stored in a server database and used as the basis for identity authentication. The front-end smart cards served as a secondary source and stored only a small amount of the identity information.

The online face-recognition system proposed in this study employs a support vector model (SVM) classifier and has the following advantages: (i) It provides privacy protection by classifying users by using a signature-based SVM classifier (SVC) based on multilevel wavelet transformation; multilevel wavelet transformation, which is also used in the face image approach, involves using a spatially enhanced local binary pattern (LBP) (Mirza et al. 2013) of a user feature and enables accurately determining the user identity in online transactions. (ii) The proposed scheme uses a complete face image rather than partial image information to increase the recognition precision. (iii) The multilevel wavelet transformation of the face images enables the system to perform hierarchical decision-making, which increases the flexibility of the system. Experimental results reveal that the proposed system provides a secure approach for protecting a user's biometric privacy and achieves high-precision face recognition, features that are crucial in e-commerce security mechanisms.

The remainder of this paper is organised as follows: Section 2 reviews previous studies in the fields of face recognition and ML. Section 3 introduces the model that was used to construct the proposed recognition system. In Section 4, the proposed approach is presented by considering the case of a user with various facial expressions, and the approach is demonstrated by employing it in an e-commerce security system. Section 5 examines the Radial Basis Function (RBF) kernel function for using the SVM approach in the proposed approach. Finally, Section 6 provides concluding remarks.

2. Relate work

This section reviews the use of three crucial techniques—SVMs, face-recognition schemes for user authentication, and wavelet transforms—applied in face recognition for biometric authentication.

2.1. Support vector models

SVMs are used for clustering data into two categories according to maximum boundary geometry. SVMs are supervised learning models associated with learning algorithms, and they are used to analyse data and recognise patterns. Generally, the results from SVM classification algorithms are more accurate than those derived from other ML approaches involving nonoptimised search methods, such as those involving artificial neural networks, least squares, k-nearest neighbour, Bayesian probability, and classification and regression trees, particularly when collect only limited training data. In an SVM training algorithm, examples are assigned to a category depending on whether nonlinear or linear binary classifiers are obtained from a set of training examples. SVMs have been shown to be useful tools for performing clustering and classification analyses (An and Liang 2013, Abe 2015). In particular, SVM theory has been developed gradually from linear SVCs to hyperplane classifiers (Devi et al. 2015); in other words, SVMs can efficiently perform nonlinear classification by using a kernel function, and their inputs can be mapped into high-dimensional feature spaces by selecting an appropriate kernel function. Furthermore, a favourable classification result is achieved by using a hyperplane that is the farthest from the nearest training data point of any class (Wikipedia 2015). The basic SVM theory is as follows (Vapnik 1995).

Consider a given training dataset $D(x_i, y_i)$, where x_i denotes n observations of malware signatures ($x_i \in R^N, i = 1, \ldots, N$) and y_i is the corresponding class label of which the value is either 1 or −1 (i.e., malicious or benign); in other words, y_i indicates the class to which the point x_i belongs, with $y_i \in \{1, -1\}$, and a y_i is assigned to each observation x_i. Each facial feature x_i is of dimension d, which corresponds to the number of propositional variables.

$$D = \{(x_i y_i)|x_{i,} \in R^N, y_i \in \{1, -1\}\}_{i=1}^{N} \quad (1)$$

A typical clustering problem is the determination of the maximum margin of a hyperplane that divides the points corresponding to $y_i = 1$ from those corresponding to $y_i = -1$. Any hyperplane can be written as the set of points x satisfying the following formula:

$$w.x_i + b = 0 \quad \forall i \quad (2)$$

where the dot in the first term denotes the dot product and W denotes the normal vector of the hyperplane. The parameter $\frac{b}{||w||}$ determines the offset of the hyperplane from the origin in the direction of the normal vector W. Generally, a decision function $D(x_i)$ is defined for clustering, with $D(x_i) = w.x_i + b$.

As shown in Fig. 1, the Lagrange multiplier in the dual optimisation theory was used to determine the maximal and minimal optimisation functions, which provided a viable solution. To solve the problem of identifying the maximum margin of a hyperplane, the Lagrange function is expressed as follows:

$$L_P = L(w, l) = \frac{||w||^2}{2} - \sum_{i=1}^{N} l_i[y_i(w.x_i) + b] - \sum_{i=1}^{N} l_i \quad (3)$$

where l_i represents the Lagrange parameter. Theoretically, solving the problem of maximising the geometric boundary requires seeking the minimum of the normal $|w^2|$, which can be transformed to minimise the Lagrange optimisation function L_p subject to the constraint $y_i(w.x_i) + b - 1 \geqslant 0$:

$$MIN\, L_P \quad \forall i$$

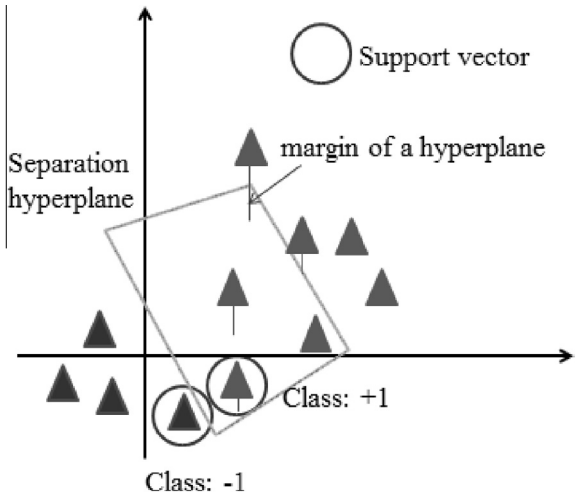

Fig. 1. Determination of the maximum margin of a hyperplane (Wikipedia 2015).