Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.735 – 738

REVIEW ARTICLE

Review on Authentication Mechanisms of Digital Signatures used for Certification

Shraddha Kulkarni[1], Prof. Vikrant Chole[2], Prof. P S Prasad[3]

[1] Department of Computer Science and Engineering, G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

[2] Department of Computer Science and Engineering, G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

[3] Department of Information Technology, Priyadarshani College of Engineering, Nagpur, India

[1] shraddha.kulkarni6@gmail.com; [2] vikrantchole@gmail.com

Abstract— Signatures are commonly used for certifying multiple financial documents such as payment receipt, cheques, stamp papers, agreement, contracts etc. as well as for personal identification such as Identity cards, marks cards etc. Since these documents usually involve transaction of money and identity verification, the signatures should be authenticated for their genuineness. In this paper, we clarify on importance of digital signature for certification as well as a review on multiple digital signature authentication mechanisms. This review helps us to proceed in the right direction of research in digital signature verification and authentication.

Keywords— Certifying; Verification; Genuineness; Authentication; mechanisms

I. INTRODUCTION

Since long past in our society, one of the common means for a person to identify and authenticate himself either to another person or to a machine is by using his signature.

Being one of the primitive ways, it is known that hand written signatures vary person to person; hence it is possible to detect any alteration or forgery to a signature.

Apart from signature, some of the recent electronic identification biometric methods include fingerprint scanning, face recognition, DNA, Palm print, hand geometry, iris recognition, retina etc. Signature as well is an important biometric attribute of a person. And the migration from traditional pen-and-paper signature to signature captured electronically is easier.

There are a lot ways to recognize a signature with lot of scope of research. One general classification being:

- ➔ Online Signature.
- ➔ Offline Signature.

Online means capturing signature directly on a device and offline means storing a paper signature electronically.

Here is an attempt to study some of the techniques used for offline signature verification.

A signature need not be always a plain text; it usually consists of unreadable special characters. Also there can be a lot of interpersonal and intrapersonal variations. These characteristics of a signature require it to be treated as an image than just a set of characters [1].

Signature recognition involves identity verification by comparing test signature against sample signatures in database. Signature recognition can be closely associated to the interpretation of human handwriting to text by a machine. One of the most primitive techniques widely used for such interpretation is an Optical Character Recognition (OCR).

Typical OCR systems involve digitization of optical characters by a scanner. The preprocessing of this image takes place involving noise reduction and normalization. Now certain characteristics are extracted for classification. Then by grouping of the extracted characters, the original symbol string is reconstructed. This context would then be applied for correction or detection of errors.

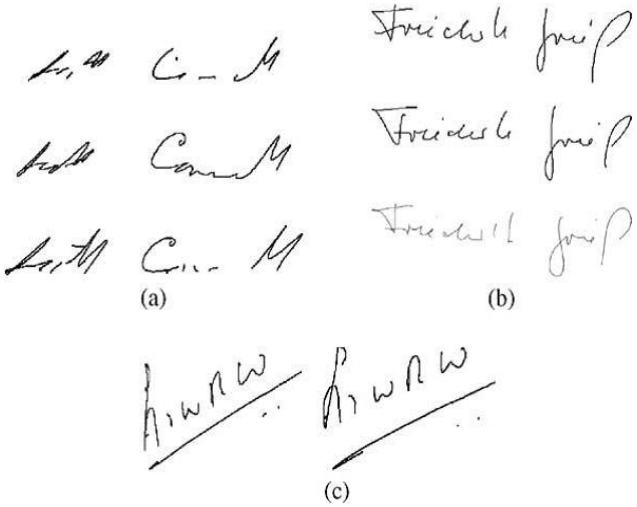

Fig. 1 Signature Samples

Although signature verification pose challenges when it comes to pattern recognition. The complexity arises due to intra-class variations i.e. one person can sign slightly differently every time (e.g. Fig. 1). Signature authenticity can be difficult to determine even for forensic experts. Also, it is not very difficult to forge a signature compared to other biometric techniques.

II. CURRENT APPROACHES

There are multiple techniques used for signature verification and they differ in either feature extraction types or the training method or their model for classification and verification:

- ➔ Hidden Markov Models Approach.
- ➔ Neural Network Approach.
- ➔ Support Vector Machine
- ➔ Template Matching Approach.
- ➔ Statistical Approach.

III. RELATED WORK

Paper [5] describes the design and development of an offline signature verification system that is based on Hidden Markov Modelling (HMM) technique performed on a series of a localized direction features extracted from a scanned signature image. In Paper [7] there is an effort to describe how a HMM are stochastic models and they have ability to acquire pattern differences and similarities. It also describes the analysis of the testing results by varying the number of HMM states and their state transition topology. The testing reported in this paper has been carried out on signature samples of 100 users which contain both their genuine as well as their skilled and random forged signature samples counterparts. The chosen algorithm in this paper is simple to be implemented which results in fast verification operation, and at the same time is reliable in detecting forgeries.

Paper[8] describes that the neural network is widely used approach because of their simplicity and power of usage. It involves, firstly extracting a feature set representing the signature and in second step involves finding out the relationship between signature and its class. Once this relationship has been detected, it gives results proposing test signature belongs to a particular signer. Paper [9] attempts to study 2 specific approaches. The objective is to determine the class and match the signature. First method is The Resilient Back propagation (RBP) neural network and second on being Radial Basic Function (RBF). A database of around 2K signatures containing 40% genuine and 60% forgeries is used. These two classifiers register 91% and 88 % success rates.

Paper [8]also elaborates on the Support Vector Machines (SVMs). These are machine learning algorithms. These algorithms use a high dimensional feature space to derive unseen data by arbitrating differences between classes of given data. Various attributes of signature such as grid features and directional are used.

Paper [10] proposes that one of the simpler approaches is the template matching approach. It is not only a very primitive approach but also easy and robust for pattern recognition. Although not all is well, its robustness does pose a numerous disadvantages. In case the patterns are distorted then it fails in signature recognition. In signatures patterns there are often large intra class variations. Nevertheless detection of light distortion will be successful. But for adept ones it would not be advisable. Geometric feature extraction, stroke analysis and graphics matching are several forms in which template matching techniques are available.

Paper [10] puts some light on another approach called the statistical approach; this approach considers each pattern as d features and considers it as a point in a d-dimensional space. In this approach pattern vectors categorized separately when represented in a d-dimensional feature space should be employed in close and disjoint regions. A feature set is considered useful if patterns from different classes are well detached. Some of the very popular example for the statistical approach is Hidden Markov Model (HMM) and Bayesian which are used for pattern recognition. What differentiates statistical approach from the template matching approach is that not only the lightly faked signatures but even the adept forgeries do not pass and are caught.

IV. EVALUATION

Analysis is drawn from comparative study of each of approaches shown in table 1

Sr. No.	Approaches	Advantages	Disadvantages
1.	Hidden Markov Model	Simple to implement which result in fast verification operation	It is Expensive approach
2.	Neural Network Approach	It is widely used approach because of its simplicity and power of usage	Neural Network cannot be retrained .If you add data later.
3.	Support Vector Machine Approach	These approach use high dimensional feature space to drive unseen data	Lack of transparency of result
4.	Template matching Approach	It is easy and robust	It can detect only unskilled forgery but fails in case of skilled forgery
5.	Statistical Approach	It is widely used and can detect skilled forgery as well	It is also expensive

V. APPLICATIONS

- Indian Patents Office.
- Directorate General of foreign trade.
- E-Procurement.
- Banking.
- Bill Payment etc.

VI. CONCLUSION

In this review we understood the importance of signature as a certification mechanism and also why is there a need for migration to digital signatures and also its authentication. We also realized the complexity of recognizing a digital signature. Digital signature verification is a complex challenge and an attempt was made to compare some of the existing schemes. This comparison study will prove a good base for further research in the area of digital signature verification. Additionally, some of algorithms which are common such as pre-processing and feature extraction can be reused. In this way we can achieve the goal of building a robust and easy digital signature verification system.

REFERENCES

[1] Velez, J.F., A. Sanchez and A.B. Moreno, 2003. *Robust off-line signature verification using compression networks and positional cuttings*. Proceedings of 2003 IEEE Signal Processing Society Workshop on Neural Networks, 17-19September, 2003, Toulouse, France, pp: 627-636.

[2] Blumenstein. S. Armand., *Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification*, International Joint Conference on Neural Networks, 2007.

[3] S.Srihari. K. M. Kalera. and A. XU, *Offline Signature Verification and Identification Using Distance Statistics*, International Journal of Pattern Recognition And Artificial Intelligence, 2008.

[4] S. Enturk. E. O¨ zgunduz. and E. Karshgil, "*Handwritten Signature Verification Using Image Invariants and Dynamic Features*," Proceedings of the 13th European Signal Processing Conference EUSIPCO 2005,Antalya Turkey, 4th-8th September, 2000nr.

[5] Bakri, Nurhaniza B. T.; Syed Ahmsinatured, Sharifah Mumtaza h; Shak *"Offline digital signature verification using hidden markov mode"l* feb-march 2010.

[6] Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, and AarónOrdóñez "*Robustness of Offline Signature Verification Based on grey level feature*" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2012.

[7] Pradeep Kumar,Shekhar Singh "*Hand Written Signature Recognition &Verificationusing Neural Network*" march 2013.

[8] Ashwini Pansare, Shalini Bhatia "*Handwritten Signature Verification using Neural Network*" January 2012.

[9] H. S. Srihari and M. Beall, "*Signature Verifcation Using Kolmogrov Smirnov Statistic*" Proceedings of International Graphonomics Society, Salemo Italy, pp. 152–156, june,2005.

[10] HemantaSaikiaand Kanak Chandra Sarma "*Approaches and Issues in Offline Signature verification System*", International Journal of Computer Applications (0975 – 8887)Volume 42– No.16, March 2012.

[11] Ramachandra A. C ,Jyoti shrinivas Rao "*Robust Offline signature verification based on global features*" IEEE International Advance Computing Conference ,2009.

[12] Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. *Parameterization of a forgery Handwritten Signature Verification using SVM*. IEEE 38thAnnual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196.

