Authenticated Document Management System

P. Anup Krishna

Research Scholar at Bharathiar University, Coimbatore, Tamilnadu

Dr. Sudheer Marar

Head of Department, Faculty of Computer Applications, Nehru College of Engineering & Research Centre. Thriuvilvamala, Thrissur, Kerala.

Abstract: *Authenticated Document Management System (ADMS) is a novel technology suggested to create authenticated digital documents where the identity of the creator as well as the users of a digital content is captured and stored with the digital content thereby ensuring non-repudiation and history information about the digital content. Various authentication techniques are currently available for digital contents like water-marking, digital signature, token systems etc. But the drawback of these technologies is that they do not refer to the creator or the user of the digital content directly. The paper suggests a mechanism of embedding the physical characteristics of human beings (bio-metrics concentrating on finger-prints) with the digital contents and thereby to create a new type of authenticated digital content where the identity of the creator as well as the users of the digital content is preserved whereby the creator cannot deny the creation of the digital content and the user cannot deny the use of the digital content.*

Keywords- Authenticated Document Management System, Biometrics, Client-Server**,** Authentic Document Format (.adf).

1. INTRODUCTION

Traditionally, the medium of a document was paper and the information was applied to it using ink, either by hand or by a mechanical process such as a printing press. Documents are often the focus and concern of business and government administration. The concerns regarding the identity/authenticity of documents in paper are managed by Signatures, Thump impressions and Seals. Till today the mechanism remains unchanged. A handwritten signature work describes the work as readily identifying its creator. The traditional function of a signature is evidential: it is to give evidence of:

1) The provenance of the document (identity)
2) The intention (will) of an individual with regard to that document

Modern electronic means of storing and displaying documents include desktop computer optionally with a printer to obtain a hard copy, Personal digital assistant (PDA), dedicated e-book device, electronic paper etc has brought forward various concerns regarding the identity/authenticity of the digital contents. Digital documents usually have to adhere to a specific file format in order to be useful. Various mechanisms, like Digital Signatures which uses cryptography in authenticating the digital contents to water-marking where a digital sign of the author/creator is embedded in the digital

content, that has been introduced to identify/authenticate digital contents had to an extend succeeded in authenticating/identifying the digital contents to its creators. But the major issue of revealing the identity of the creator of the digital content still remains in case of digital documents. As all the above technologies are mainly concentrating on few formats of digital data and transactions and more over the users involved in the digital system are not directly referred by the system. Now with the flourishing of the computer aided biometric technology it has become possible to refer/related a user directly in a digital system by capturing the bio-metric information of the user and managing the same in the digital system. The difference between the biometric information to the other existing technologies lays in the fact that bio-metric information is something that the user has with him as his personal attributes while all the other existing technologies like digital signature, tokens etc is something which the user knows or can control and which is not integral part of him and is something external.

1.1 BIOMETRICS

One of the most popular signature namely Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided in two main classes:

1) Physiological which are related to the shape of the body. Eg. Fingerprint, face, DNA, Palm print, hand geometry, iris, retina, odour/scent etc.
2) Behavioural which are related to the behaviour of a person. Eg. Typing rhythm, gait, and voice etc.

A biometric computer system can operate in the following two modes:

i) Verification – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.

ii) Identification – A one to many comparisons of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

1.2 AUTHENTICATION

Authentication is the process of verifying the identity of a user in relation to a “document”. Currently there are various methods applied in authenticating the digital contents. All methods imply certain considerations to be followed like non-repudiation, privacy, confidentiality, integrity of information etc. The identity of a user can be verified by something unique to the individual (like physical/biometric features), something the individual knows (like passwords, pins etc), something the individual possesses (like token,

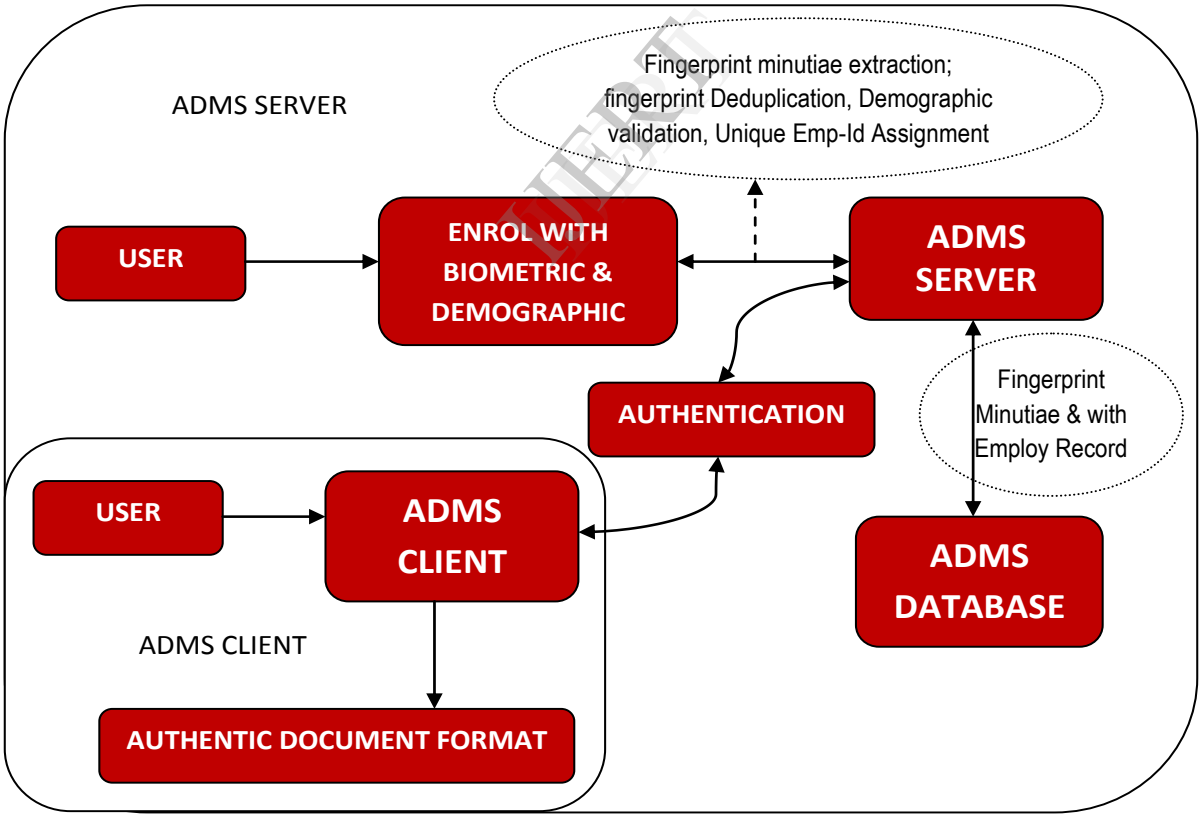
digital signatures etc). Visual signature verification was once the sole method to verify identity of a document. Now the same has been replaced by digital signatures, tokens etc. The paper suggests the using biometrics in authenticating the digital contents.

2. AUTHENTICATED DOCUMENT MANAGEMENT SYSTEM

The research is to develop application software (ADMS) that binds the digital documents created by a user with his biometrics (especially fingerprint) and to create an authenticated document which is legally valid throughout the organization. The system will run on a client-server model, where considering a single organization there will be an ADMS server which will hold the biometric details of all the concerned staffs/users of the system and will validate and authenticate the users in the client systems for using ADMS client and creating/editing/viewing authenticated documents. The ADMS comprises of two main components.

1) The ADMS Client Server Application
2) The Authentic Document format (.adf).

2.1. THE ADMS CLIENT SERVER APPLICATION MODEL

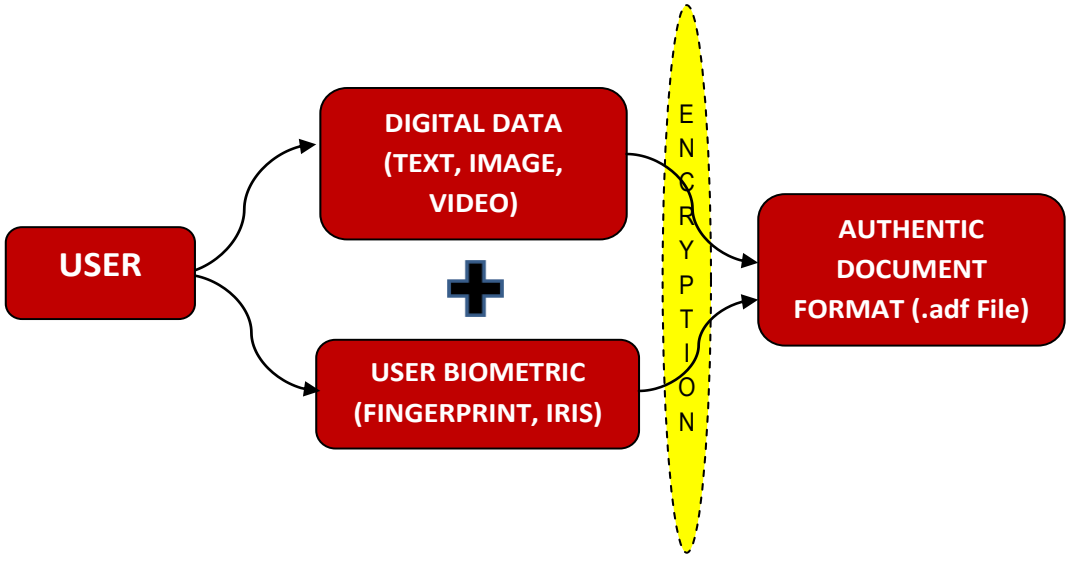


The above model describes the complete workflow of creating an ADMS for an organization. The ADMS SERVER application will be running as the central Verification, Validation, and Administration server of the organization. The ADMS SERVER application will have functionalities to enrol a user to the system by capturing his fingerprints, extracting the

minutiae, encryption and decryption of minutiae data, doing a Deduplication with the existing employ records, validating the demographic information's of the employ, finally assigning a unique employ-id to the employ and saving his biometric information along with the demographic data in the ADMS database. Administrative roles include removing a user, updating a user, report generation, etc.

The ADMS Client is basically an authentic text processing tool with advanced login authentication with fingerprints and also with the ability to create the Authentic Document Format by embedding/mixing the fingerprints of the user with the digital content created by the user. The ADMS Client works with the ADMS Server for the creation of the Authentic Document. To login to the ADMS client the user needs to have login credentials. After providing the login credentials he need to give his fingerprints for authenticating with the ADMS Server. Once the ADMS Server gives an Authentication success, the user is allowed to login to the client and can start to create an authentic digital content. After the contents are typed / entered, the user needs to save the content. During this phase of work also the ADMS Client requires the user to provide his fingerprints and get authenticated by the ADMS Server. Once authenticated successfully the ADMS Client will integrate/embedded/mix the user biometric information with the data using a separate ADF Algorithm and encrypt the same to create the Authentic Document Format (.adf File). The Authentic Document Format (.adf File) once created is a normal file which can be transferred over media/internet as any other file, but needs the ADMS at the receiving end for the operation/processing of the same. The implementation also takes care of creating the .adf File in such a manner that, it can be opened / edited only by the ADMS Software and not by any other computer application including notepad. The ADMS Client will authenticate all the users who can use the application with their physical attributes (finger print). First it authenticates the person with the ADMS Server to start the application, then allows for text editing and finally before saving the document it again ask for the finger print, then authenticates with the ADMS Server and finally creates an Authentic Document (.adf proposed extension for the file format) which is encrypted and merged with the finger print minutiae values and the textual data.

2.2 THE AUTHENTIC DOCUMENT FORMAT (.adf File)



The Authentic Document is created by the ADMS Client by embedding/mixing and encrypting the user biometric with the user data using the ADF Algorithm and creating a new Authentic Document Format (.adf File) which carries the user biometric along with the user data. The successive updations/actions on the Authentic Document will also be recorded hence creating a history for the digital content. Once the concept is implemented those paper works which need review at various levels in an organization can be replaced by the ADMS Authentic Document Format and also the same will lead to various levels of innovations in the work culture and life presently available on earth.

3. CONCLUSION & FUTURE WORK

The research is to develop application software (ADMS) that binds the digital documents created by a user with his biometrics (especially fingerprint) and to create an authenticated document which is legally valid throughout the organization. The system will help to enrol the user with his/her biometrics and then to create/edit/view authenticated documents. The system will run on a client-server model, where considering a single organization there will be an ADMS server which will hold the biometric details of all the concerned staffs/users of the system and will validate and authenticate the users in the client systems for using ADMS client and creating/editing/viewing authenticated documents. In future, each of the ADMS Server can again be linked to the Unique Identification System of the Nation for a nationwide Authenticated Document System. Once the system is in place, it will be a great step forward in creating an eco-friendly, paperless offices, with majority authenticated digital contents which is having total legal validity globally. The key areas of concern while designing the system is related to privacy, security, biometric comparison algorithms, data encryption/decryption algorithms, implementation of biometric technology nationally, IT Law modification and legal validity of digital contents and consistency of the biometric system etc.

REFERENCES

1) Document Identity, Authentication and Ownership: The Future of Biometric Verification, M.C.Fairhurst Department of Electronics, University of Kent, Canterbury, Kent CT2 7NT, UK Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03) 0-7695-1960-1/03 $17.00 © 2003 IEEE
2) Signature Detection And Matching For Document Image Retrieval, Guangyu Zhu, Student Member, IEEE, Yefeng Zheng, Member, IEEE,David Doermann, Member, IEEE, And Stefan Jaeger, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 31, NO. 11, NOVEMBER 2009
3) Offline General Handwritten Word Recognition Using an Approximate BEAM Matching Algorithm, John T. Favata, Member, IEEE, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 23, NO. 9, SEPTEMBER 2001
4) Embedding Biometric Watermark on Document Image using Discrete Wavelet Transform, Ioi-Tun Lam and Chi-Man Pun, Proceedings of the 2009 IEEE International Conference on Information and Automation June 22 -25, 2009, Zhuhai/Macau, China
5) Electronic Contracts, P. Radha Krishna • Infosys Technologies, India, Kamalakar Karlapalem • International Institute of Information Technology, India, 1089-7801/08/$25.00 © 2008 IEEE
6) Encyclopaedia of Bio-metrics, Stan.Z.Li, Springer, ISBN: 978-0-387-73002-8

AUTHOR PROFILE

P.Anup Krishna is an IT professional having 12+ years experience in Software Applications/Technology Management. Currently he is engaged with AvK Innovative, Kerala, India as IT Manager. He has a Masters degree in Information Systems. He is currently pursuing Ph.D in Bharathiar University, Coimbatore, India

Dr. Sudheer S Marar is an Associate Professor and HoD of the Department of Computer Applications at Nehru College of Engineering and Research Centre. He holds three Masters Degrees in Computer Applications, Business Administration and Information Technology. For his research in Socio-Technological aspects at RR Academy of Higher Learning and Research Chennai, he was awarded a PhD by University of Honolulu USA. His research interests include Data Modelling, Technology Management and Socio-Technological features.