Enhancement of IRIS Authentication Model for e-commerce using RSA Algorithm

Tannia Rubavathy Glory Manova[1], Rajan John[2]

Abstract. E-Commerce is an outcome of globalization and technology outbreak of the 21st century. The consistency on internet privacy protection plays a major role to boost the growth of e-commerce. E-commerce industry is slowly addressing security issues on their internal networks. But security protection for the consumers is still in its infancy stage posing a harrier to the development of e-commerce. There is a growing need for a combination of legislation and technical solutions to globally secure customer privacy. The US Federal Trade Commission has identified the need for defining privacy policies to address consumer data security. A technology solution using biometric technique is proposed for preventing identity theft and false authentication in the course of e-commerce transactions. This research proposes a web-based architecture to use encrypted iris patterns as biometric attribute for authentication of a customer for e-commerce transactions, because iris patterns are unique to an individual.

Key Notes- authentication, biometric, e-commerce, iris verification, RSA algorithm

1. INTRODUCTION

SECURITY is becoming an increasingly important issue for business, and with it comes the need for appropriate authentication; consequently, it is becoming gradually more important to develop secure e-commerce systems. Fraud via the web, identity theft, and phishing are raising concerns for users and financial organisations. In addition, current authentication methods, like passwords, have many problems (e.g. some users write them down, they forget them, or they make them easy to hack). We can overcome these drawbacks by using biometric authentication systems. Biometric systems are being used for personal authentication in response to the rising issue of authentication and security. Biometrics provides much promise, in terms of preserving our identities without the inconvenience of carrying ID cards and/or remembering passwords. This research is important because the securing of e-commerce transactions is becoming increasingly important. Identity theft, hacking and viruses are growing threats to Internet users. As more people use the Internet, more identity theft cases are being reported. This could harm not only the users, but also the reputation of the organisations whose names are used in these illegal acts. There are several methods to capture the iris features. Gabor filter is used in several works [1], [2], [3]. In [4], zero crossing wavelet transforms used to extract the iris features. The other methods for iris feature extraction include Log-Gabor wavelet [5], Haarwavelet [6], [7], Laplacian-of-Gaussian filter [8], Hermitte Gaussian- moments [9] etc. It is reviewed that the number of extracted iris features in the existing work is very high. The existing approaches require higher number of bits to represent the iris features and as a consequence the need of higher computations to process these iris features. In this paper, we addressed the existence of standardized **iris** image capture and encryption software along with the web camera that is built in the recent computer systems. The figure.1 shows System architecture

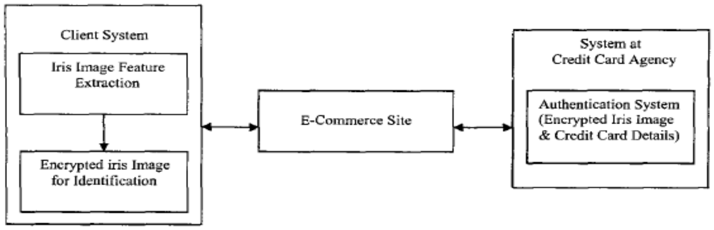
Client System
Iris Image Feature Extraction
Encrypted iris Image for Identification
E-Commerce Site
System at Credit Card Agency
Authentication System (Encrypted Iris Image & Credit Card Details)

Fig.1: System Architecture

2. PROBLEM RECOGNITION

E-commerce industry is slowly addressing security issues on their internal networks. But security protection for the consumers is still in its infancy stage posing a harrier to the development of e-commerce, since internet is international and globally unregulated there is an acute need for consumer privacy protection. In a global market place the laws of one country do not apply to transactions originating or taking place in other countries. Preventing identity thief and false authentication in the course of e-commerce transactions. This research proposes a web-based architecture to use encrypted iris patterns as biometric attribute for authentication of a customer for e-commerce transactions, because iris patterns are unique to an individual.

3. PROPOSED SYSTEM

Preventing identity thief and false authentication in the course of e-commerce transactions. This research proposes a web-based architecture to use encrypted iris patterns as biometric attribute for authentication of a customer for e-commerce transactions, because iris patterns are unique to an individual. On the server system an iris image of an individual was captured, preprocessed and key features extracted using the principal components analysis technique. The resulting data set was stored as a string data type in a database consisting of the individual's name, credit card details etc. On the client system, the same individual's iris image was processed and key features extracted in a similar way using PCA, and the resulting dataset was encrypted and sent to the server machine. On the server machine, the encrypted data set was decrypted and the dataset was compared with the already existing dataset in the database. The individual was authenticated as there was no mismatch. Same dataset was compared with the dataset resulting from the iris of a different person, there was a mismatch. Hence the person was not authenticated and effectively resulting in the cancellation of the e-commerce transaction.

4. ENCRYPTION / DECRYPTION OF DATA

The RSA algorithm can be used for public key encryption. The 3 basic steps of this algorithm are: Key Generation Algorithm, Encryption and Decryption

4.1 Key Generation Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.

2. Compute n = pq and (ϕ) phi = (p-1)(q-1).

3. Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1.

4. Compute the secret exponent d, 1 < d < phi, such that ed =1 (mod phi).

5. The public key is (n, e) and the private key is (n, d). The values of p, q, and phi should also be kept secret.

Where, n is known as the modulus.

e is known as the public exponent or encryption exponent.

d is known as the secret exponent or decryption exponent.

4.2 Encryption

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).

2. Represents the plaintext message as a positive integer m.

3. Computes the ciphertext c = m^e mod n.

4. Sends the ciphertext c to B.

4.3 Decryption

Recipient B does the following:-

Uses his private key (n, d) to compute m = c^d mod n.

Extracts the plaintext from the integer representative m.

4.4. Iris Recognition Algorithm Based on PCA

In iris image synthesis, an iris recognition based on PCA is first presented to put iris synthesis in context. Most existing iris recognition methods are based on the local properties. as phase, shape, and so on. However, iris image synthesis based on local properties is difficult to implement. Recently, Bae et al. attempted to use the Independent Component Analysis (ICA) to extract iris feature. and PCA can all be used for global feature extraction, PCA has superiority in image construction, because we can control the construction errors by selecting the cumulative variance. Euclidean distance and nearest neighborhood (NN) classifier are adopted here.

When should PCA be used?

- In community ecology, PCA is useful for summarizing variables whose relationships are approximately linear or at least monotonic

e.g. A PCA of many soil properties might be used to extract a few components that summarize main dimensions of soil variation

- PCA is generally NOT useful for ordinating community data

- Why? Because relationships among species are highly nonlinear.

5. REQUIREMENT ANALYSIS

The biometric credit debit card authentication system consists of iris image feature extraction, RSA encryption unit at the client side with a decryption unit along with database consisting of credit debit card details at the server side for authentication. A web camera integrated into the client system takes a picture of the eyes of the user who is doing an e-commerce transaction, and he or she must be authenticated by the credit debit card agency for the transaction to proceed. An algorithm is developed to extract the iris image from the preprocessed picture by applying the principal components analysis technique. By using the RSA algorithm the extracted features are encrypted and transmitted to the e-commerce site along with credit debit card number, name, and expiration date. This information is authenticated by the credit debit card agency for the e-commerce site to allow the user to proceed with the transaction. Since the iris image is encrypted before sending to the e-commerce site the private information of the individual is protected and only the credit debit card agency has access to it.

6. FEASIBILITY STUDY

Feasibility study was conducted on the candidate system to check whether it can proceed with the new system. This Study identifies, describes and evaluates the candidate systems and Select the best system for the job.

6.1 Economic feasibility

Economic feasibility is the most frequently used method for evaluating the effectiveness of a new system. The procedure is to determine the benefits of savings that are expected from a candidate system and compare them with costs. If benefit outweighs costs, then the decisions are made to design and implement the system. Though initial investment is high the benefits that will be reaped in along the term is high. Since the new system is developing in client/server environment it is user-friendly to work with and since it also removes the drawback of the existing system it was considered economically feasible to proceed with the system.

6.2 Technical feasibility

Technical feasibility centers on the system and what extent it can support the proposed addition. This involves financial consideration to accommodate technical enhancements. If the budget is the series constraint then the project is judged not feasible. The hardware requirements for the new system are the client is ready to install the necessary software like, so the system was considered technically to proceed with.

7. TESTING PROCESS

Software testing is a crucial element of software quality assurance and represents the review of the specification, design and coding. The user tests the developed system and changes are made according their needs. The testing phase involved the testing developed system using various kinds of data. System testing is the stage of implementation that is aimed at assuring that the system works accurately and efficiently before live operation commences. Testing is the vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be successfully achieved. Here there are two testing methods; they are white box testing and Black box testing.

7.1 White Box Testing

This will be tested at the outside of the environment. This means accessing the server. i.e., accessing data from the database. This will check whether data is retrieved correctly or not will be seen. Here MYSQL server will be used as backend database. Here for the project some tables are created, In the program it has clearly specified. Whenever inserting data, updating data and selecting data from the database the queries must be written carefully. The separation between the string and numeric must be shown. The client side validations will be written in PHP so that the data entered is numbered or string.

7.2 Black Box Testing

This is another important test method will check only internal code loops, conditional loops will be checked. This method will check the loops like FOR…LOOPS, WHILE…LOOP all will be checked their boundary condition also. If the data at extreme conditions are correctly retrieved. So there will be no error.

CONCLUSIONS

In this paper, an attempt has been made for a technology solution based on the uniqueness of iris image as a biometric, for customer identification and authentication to secure e-commerce transactions. This is a very effective and robust method for preventing credit card fraud when making e-commerce transactions. Research leading to this application using iris image as a biometric is very premature at this time. Standards are yet to be established to capture high quality iris images. The PCA technique is a good method for processing and extraction of key features of iris image and not difficult to implement compared to other feature extraction techniques like discrete wavelet transform etc. Complex algorithms for encryption and decryption may be researched. The growth of e-commerce is purely dependent on customer huts for secure transactions. Global security laws and technology solutions will contribute towards this goal.

Limitations

A software need to be present in all the client systems so that while doing e-commerce transactions, the ins image of the individual can also be captured, encrypted and sent along with the name, credit debit card number, and, expiration date. At the time of transaction the iris image of the customer is captured using a web camera built in the client system. This project necessitates the existence of standardized **iris** image capture and encryption software along with the web camera that is built in the recent computer systems.

Acknowledgment

I take this privilege to express few words of gratitude and respect to all those who helped me in completing this project.I thank the God Almighty for giving me the opportunity of doing this project work successfully. My heartfelt thanks to my **Parents** for their invaluable support in doing this project. I express my heart filled sincere gratitude to **Rev.Sr.A.Fatima Antony**, the Principal of Fatima College. It's my sincere thanks to **Mrs.B.Chandirika, M.C.A, and M.Phil.** Head of the Department of Computer Applications helped me a lot to do the project efficiently. It's my duty to thank other staff members of Department of Computer Applications for their kind cooperation to do this project. I wish to Special thanks for Assistant Dean of Research **Dr. RAJAN JOHN** for helping me to complete my project successfully. I wish to thank everyone who has helped me directly or indirectly for the successful completion of the project work.

About Authors

Dr. RAJAN JOHN received his MCA degree from Karunya University and has completed his **Ph.D** from Karunya University, Coimbatore. He has also published more than 20 research papers at National and International level. He has given more than 20 seminars at Karunya University, All Nations University, and IEEE etc. He has more than 10 years of teaching experience at Graduate and Post Graduate level. Guided several projects of UG Students ofComp. Sc. in various areas like data mining, Research Methodology and OOPS. He is presently working as the Assitant Dean (R&D) & professor of Computer Science Department, All Nations University College in Koforidua, Eastern Region, Ghana-West Africa.

Miss. **Tannia Rubavathy Glory Manova** received B.sc from Madurai Kamaraj University, Madurai, India, in Computer science in the year 2006 and later did her MCA in Fatima College, Madurai Kamaraj University Madurai, India. Currently she is working as an All Nations University College in Department of Computer Science and Engineering, Koforidua, India. She has participated more in reputed national and international conferences. Her area of interest includes, Computer organization, Digital computer Fundamentals, Visual basics and Java Programming.

REFERENCES

[1] R.Raghavendra, Ashok Rao, Hemantha Kumar, “Multimodal Biometric Score Fusion using Gaussian Mixture Model and Monte Carlo Method, Special issue on Advances in Machine Learning and its application,” *International Journal of Computer science and Technology(JCST), Springer.*

[2] Ramasamy Palaniappan, Danilo P. Mandic, “EEG Based Biometric Framework for Automatic Identity Verification”, *Journal of VLSI signal processing*, 49, 2007, PP: 243-250.

[3] HU Jian-feng, “Biometric System based on EEG Signals by feature combination, *International Conference on Measuring Technology and Mechatronics Automation, IEEE Computer Society*, 2010, PP: 752-755.

[4] Tieniu Tan Yuchun Fang and Yunhong Wang “Fusion of global and local features for face verification”, *In 16th International Conference on Pattern recognition*, 2002.

[5] R. Raghavendra, Ashok Rao, Hemantha Kumar, “Multisensor Biometric Evidence Fusion of Face and Palmprint for Person Authentication using Particle Swarm Optimization (PSO)”,*International Journal of Biometrics*, 2010, Vol.2, No.1,PP: 19–33.

[6] Kumar, A. Hanmandlu, M. ; Kuldeep, M. ; “Automatic Ear Detection for Online Biometric Applications” ,
International conferenceon Image processing, India.

[7] Ms.Lenina Vithalrao Birgale, Manesh Kokare, **“**Iris Recognition Using Discrete Wavelet Transform”, *International Conference on Digital Image Processing,IEEE Computer Society, India.*

[8] Valery Starovoitov, Agnieszka Kitlas Golińska, Anna Predko-Maliszewska, Maciej Goliński ; "No-Reference Image Quality Assessment for Iris Biometrics", *Image Processing and Communications Challenges 4 Advances in Intelligent Systems and Computing Volume 184, 2013, pp 95-100*.

[9] Li Ma, Tieniu Tan, Dexin Zhang, Yunhong Wang, "Local Intensity Variation Analysis for Iris Recognition",
National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, Beijing, P.R. China, 100080
5 10 15 20 25.