*2012 International Conference on Information and Network Technology (ICINT 2012)*
***IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore***

# Antispoofing Model for Secure Information Retrieval in a Networking Society

Ravi Hosur [1 +], Sanjeevakumar Hatture [1] and Rashmi Karchi [2]

[1] Department of CSE, Basaweshwara Engineering College, Bagalkot, Karnataka (India)
[2] Department of MCA, Basaweshwara Engineering College, Bagalkot, Karnataka (India)

**Abstract.** The proposed model is an extension of our previously proposed model for LAN security system which can be used in all the public security system; where a new technique/scenario is embedded in the existing biometric systems to prevent the spoof attack. The model follows with by authenticating user with his details by providing multiple inputs at different stages. In the first stage (said to be the basic authentication step), the user provides the biometric details as username and password which is tested for authentication, and once if the basic details are valid, then in the next stage user need to provide a four digit random number with an answer to a random question given from a number of questions (which has been stored with answers given at the registration by the user for a set of questions). If the answer given by the user to the question is valid, then the random number will be converted into a cipher text (by using some of the standard Cryptography algorithm). Finally, the system will prompt the user to re-enter his/her password (now cipher text) to get authenticated for accessing the information from the system, on successful authentication.

**Keywords:** user authentication, biometric traits, security system, antispoofing, cipher text.

## 1. Introduction

Biometric system identifies a person based on his/her details like thumb impression (left/right), eye retina, voice, etc. No two individuals' biometrics may seem to be identical because with respect to their voice when considered vocal tract shapes, larynx sizes, and other parts of their voice production organs are different, with respect to eye retina their nervous system connected within the nervous system may be different and thumb impression the line in the fingers may vary from one to another. In addition to these physical differences, every user can also produce characteristic like manner of speaking, use of a particular accent, rhythm, intonation style, pronunciation pattern, choice of vocabulary, etc. with voice of an user, similarly with other types of biometrics. Hence the biometric systems use a number of these features in parallel, to achieve a complementary way for accurate recognition.

A spoof is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor. Differentiating a genuine biometric trait presented from a live person versus some other source is called spoof detection. The act of sensitivity *("aliveness"*) signs such as pulse is one method of spoof detection. In some areas of research, the term aliveness detection is synonymous with spoof detection. In other areas of research, aliveness detection is the more limited problem of distinguishing a live human trait from a non-live human trait and in still others aliveness detection is, very narrowly, defined as the sensing of vitality signs. Spoof detection can occur before biometric data is collected or during data processing. In a decoupled system no biometric data is collected until the spoof detection method is satisfied that a live human is present.

+ Corresponding author.
*E-mail address*: hosuravi@gmail.com.

For identifying the aliveness detection and further to authenticate user we explore the idea of biometric system which can be deployed in all public interactive and sensitive environments for strengthening the security system.

## 2. Review of Literature Survey

Most of the researchers addressed the issues in all biometric systems as a security measure by considering many scenarios where the user's biometric details of finger/palm/eye/voice (input) is perceived and is read by an interfacing/simulating device to represent them into graphical signals.

Our previously proposed model [1], was designed for LAN security system by using text-dependent speaker identification system. The system was modeled only to work in limited area like intranet or LAN system. We now extending the system for WAN system by considering the issues related to security measures concerned to internet.

In paper [2], these (Speaker) signals are measured in terms of cepstral coefficients by the selective Linear Prediction analysis method. Although identification is performed on the rich amount of speaker voice and reported performance rate of 96.8% for frequency 3 Hz and 98.6% for 4Hz. Hence, the system is meant to work well within the frequency range between 3-4Hz to get more stabilized for speaker identifications.

In paper [3], the system tabulated the results with the recorded the samples of voice (input data) in terms of talking styles like normal, shout, slow, loud, and soft depending on stress bound and stress unbound, with stress bound are better with 93% than stress unbound gives 90%. The remaining styles were recorded with less in performance

Paper [4] reported in 100% results for text-dependent Speaker Identification and 85.7 – 90.5% for text independent speakers for sentences and 100% for English digits. The paper recorded with the codebook being generated

In paper [5], to recognize and to determine the speaker the method adopts text dependent method where each speaker is represented by a sequence of vector quantization codebooks. Then these are tested with the system for single word detection and extended to multiple words detection scheme. A 10 digit code was incorporated into the recognition process and achieved a false rejection rate of 0.8% and a false acceptance rate of 1.8% on a combined database that contained 16 acceptable speakers and 111 imposters.

In the paper [6], it is investigates the three common speech coding systems namely Code Excited or Vector Excited Coders(CELP), Linear Prediction Coefficients(LPC) and Global System for Mobile(GSM) on the pitch and formant frequencies of speech extracted from several dialect regions of the TIMIT speech corpus. With all the trajectories of comparison, the time dependent fine-detailed characteristics of both source and the transfer function are significantly degraded by the speech coding.

In paper [7], works with speech and Electrocardiogram (ECG) signals using wavelet transform for cryptographic key generation based on the uniqueness and quasi-stationary behavior of ECG and speech signals for an individual. The designed system is simulated to increase the performance with a report of False Acceptance Rate (FAR) of 1.27% and a False Rejection Rate (FRR) of 10.62% for the system. The paper does not compromise with the keys of a group or a corporation that could happen in the case of maintaining a centralized database with the biometric information of all users but can compromise with the key of user hacked by the third party.

Further in the paper [8], authors proposed that variable-text, text-dependent speaker recognition systems based on one pass Dynamic Programming algorithm that used multiple templates for each word for capturing idiosyncratic intra-speaker variability of a word resulting in significant improvement in the performance by considering Closed-set-speaker identification (CSI), Speaker Verification (SV) and open-set-speaker identification (OSI) as the recognition systems. The developed system also helped to enable the speaker recognition system with continuous input utterances which produced the best results for population of 100-200 closed-set and open set speakers.

In the paper [9], the identification of speaker in an open set is by text-independent system. The results produced are better by using the Cohort normalization methods. By the experimental results, the speaker

verification is based on Gaussian Mixture Model (GMM) where the verification has proved valuable insight into certain speaker recognition characters with respect to performance features and limitations. The study has also shown that because of practical limitations, the use of the standardizations of the general cross speaker scores.

In the paper [10], for detecting the spoof fingerprint attacks in the biometric system is on the observation that, real and spoof fingerprints exhibit different textural characters based on structural, orientation roughness, smoothness and regularity differences of diverse regions in a fingerprint image where the images are captured by Local Binary Pattern(LBP) histograms. The dimensions are integrated as feature set which is reduced by running Pudil's Sequential Forward Floating Selection (SFFS) algorithm. A new image (single) based method utilizing integrated gray level texture and wavelet energy information for spoof finger detection is presented.

The paper [11], proposes a new Curvelet transform-based method to detect spoof fingerprint attacks in fingerprint biometric systems. Classification rates are achieved with various classifiers for energy signatures ranging from 94.12 to 97.41% and for concurrence signatures range from 94.35 to 98.12%. The performance of the proposed method is very promising, as only one image is sufficient to detect spoof fingerprint attacks at the sensor.

In the paper [12], features of speaker identification are defined with each feature modeled using the Gaussian Mixture Model (GMM) and construct a speaker's models dictionary that are used by the Multi-Layer Perception (MLP) classifier, the Support Vector Machine (SVM) classifier and the decision Tree (DT) classifier for matching and the scores (output) of all classifiers are then considered for combinations. The combined several classifiers applied in different features and study their use for text-independent speaker identification.

In the paper [13], wireless Local Area Networks(WLANs) that use MAC filtering to allow stations with registered MAC addresses to use the network where the attacker has many tools like AirJack, wireshark to capture the packets in WLANs and find authorized MAC address. The attacker masquerades as an authorized station and can launch denial of service attack. The work presented a power hopping technique which can be used by Access Point (AP) to discern the authorized packets from the masquerading packets and thus deny the attacker from using the system. The AP learns about the signal strength about various locations and also AP learns about the noise to signal ratio. The technique could more consumption of energy because even if the station is near AP, in order to meet expected power level, station might use more power than the optimal power needed.

The paper [14], highlights the vulnerabilities, classifying the threats and clarifying the requirements for such a dynamic framework which transfers the vulnerability evaluation results into legacy knowledge in security domain which facilitates comparison of two systems as well as definition of the threats in an independent and isolated way. This model is extremely critical and move of the current standards can address all the security concerns in this area especially with the growing knowledge of emerging spoofing techniques and helps in monitoring of security breaches and assessment of reliability of defense mechanisms.

In the paper [15], the scheme extracts the fingerprint feature of cognitive user to get the Received Signal Strength (RSS). The extracted Eigen values can be used as the input vectors of the Back Propagation (BP) Neural Network which are trained by the honest users' RSS. Simulation results shows that the scheme can effectively detect identity spoof attack with a low false alarm rate and miss alarm rate. The process extracts feature information RSS value, and classes these data through BP network.

The paper [16] exhibits a worst case scenario that the attacker is able to fabricate an exact replica of genuine biometric trait which was simulated by assuming that the matching score distribution of fake traits is identical to the one of genuine users. So the biomedical system used does make a face and fingerprint matcher whose scores are fused using the well-known sum, product, weighted sum and Like-Li-hood Ration (LLR) rules and, investigates whether a realistic spoof attack against both modalities can allow the attacker to crack multi-modal system. Results in robust and performance factors under a spoofing attack against all traits are still unacceptable for security applications. In other words, they can be cracked by spoofing all the fused traits even when he attacker is not able to fabricate an exact replica of the genuine user's traits.

In summary, the research works cited above address most of the issues on all biometric systems used in security systems by identifying the user. Further, there is a scope to address an issue on the aliveness detection in such systems whether the user is being genuine or not. Also more security can be provided to the system to avoid the intruder's attack in noisy environment and to identify the user even if the details are revealed to the third party.

## 3. Proposed System

Our proposed model can be deployed in a system where a secured data access can be made by using the biometric system. This model is introduced as a middleware between the user and the required information. The proposed system consists of three modules: User module, Biometric system module and Cipher text generation module. The proposed model is as shown in figure 1.

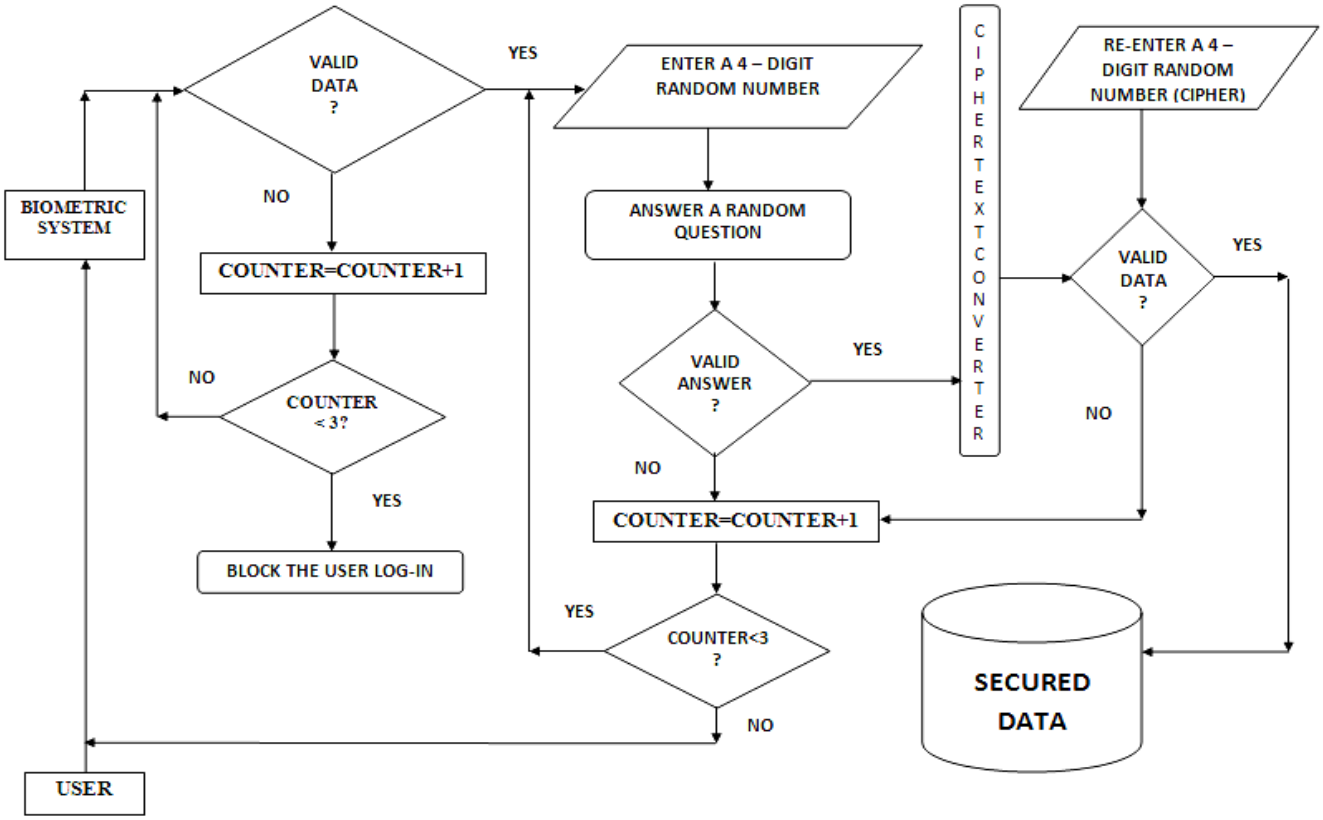


Fig. 1: Proposed Antispoofing Model

### 3.1. Working principle

The model includes number of stages. The basic validation stage where the registered user presents the initial details provided during the registration i.e., his identification details in the form username and the passwords stored as a biometric trait in the form thumb impression, eye retina scanned details, speech, etc. the registered details are given to enter into the user home page if he is genuine with all his details. If the number of attempts does not exceeds 3 then the user can try for one more time to log in to the system with his details again otherwise the user account will be blocked for the next time. If he is successful with initial step, then the user is asked to enter a 4 digit random number and then will be asked to answer a randomized question which will be given to the user during his/her registration with list of questions. These questions will be appearing randomly every-time the user wish to perform any action or after entering a 4 digit random number, where the answers of all the questions should be updated with new answers (not same as previous) every once in a month which will prevent the third party intervention and catch the details of the user that will be provided during the log in to the system. Once the user succeeds with this stage, he/she will be asked to enter a 4 digit random number that should match the 4 digit cipher text generated by the algorithm (that converts the random number to cipher). The algorithm will be explained to the user during their registration of how the cipher text will be generated. If the both (cipher and user's re-entered random number) match

then the user is allowed to access the secured information from thr database, otherwise the same process of authentication is followed.

## 4. Conclusion

The proposed Antispoofing model can be effectively deployed in existing biometric security system to prevent the spoof attack by providing the aliveness detection by prompting the user to enter the Cipher text generated by the system. Further, it authenticates the user in all biometric security based systems with better results.

## 5. References


[1] Ravi Hosur, Sanjeevakumar M Hatture and Rashmi P Karchi, " A Model to Prevent a Spoof Attack using Text-dependent Speaker Identification", proceedings of Advances in Computer Science and Information Security(ACSIS'12), 2012

[2] Shaji Hayakawa and Fumitada Itakura, "Text Dependent Speaker Recognition Using the Information In The Higher Frequency Band", IEEE ICASSP. 1994, pp I-137 to I-140

[3] Shahin, Ismail Botras, Nazeih, "Text Identification Using Hidden Markov Model with Stress Compensation Technique", Southeastcon '98, Proceedings,IEEE. 1998, pp 61-64

[4] Aliaa A. Youssif, Ebada A. Sarhan, and W.H.El_Behaidy, "Development of Auomatic Speaker Identification System", 21st National Radio Conference (NRSC2004) (NTI) March 16 – 18th, 2004

[5] Joseph T Buck, David K Burton, and John E Shore, "Text Dependent Speaker Recognition Using Vector Quantization", IEEE International Conference on (ICASSP) Acoustics, Speech, and Signal Processing. 1985, pp 391-394

[6] M Phythian, J Ingram and S Sridharan, "Effects Of Speech Coding on Text dependent Speaker Recognition", IEEE Region 10 Annual Conference on Speech and Image Technologies for Computing and Telecommunications, proceedings of IEEE. 1997, pp137-140

[7] H. A. Garcia-Baleon V. Alarcon-Aquino O. Starostenko J. F. Ramirez-Cruz, "Biomodal Biometric System for cryptographic Key Generation Using Wavelet Transform", Proceeding ENC '09 Proceedings of the 2009 Mexican International Conference on Computer Science IEEE Computer Society Washington, DC.2009 pp 185-196

[8] V Ramasubramanian, V Praveen Kumar, Deepak Vijaywargiay, D Harish, S Thiyagarajan, Amitav das, "Text Dependent Speaker Recognition systems based on One-pass dynamic programming algorithm", Speaker and Language Recogn.

[9] M. Ariyaeeinia, J. Fortuna, P. Sivakumaran and A. Malegaonkar, " Verification effectiveness in open-set speaker Identification", IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 6245.2006, Pp 618-624.

[10] Shankar Bhausaheb Nikam Suneeta Agarwal, "Texture and Wavelet-Based Spoof Fingerprint Detection for Fingerprint Biometric Systems", First International Conference on Emerging Trends in Engineering and Technology, icetet.2008, pp.675-680

[11] Shankar Bhausaheb Nikam Suneeta Agarwal, "Fingerprint Liveness Detection Using Curvet Energy and Co-occurrence Signatures", Fifth International Conference on Computer Graphics, Imaging and Visualisation. CGIV '08.2008 pp 217-222

[12] S. Zribi Boujelben, D. Ben Ayed Mezghani, N. Ellouze, "Application of Combining Classifiers for Text-Independent Speaker Identification", International Conference on Electronics, Circuits, and Systems. ICECS 2009. 16th IEEE.2009, pp 723-726

[13] Vijayakrishnan Nagarajan, Vetri Arasan, Dijiang Huang, "Using Power Hopping to Counter MAC Spoof Attacks in WLAN", Proceeding CCNC'10 Proceedings of the 7th IEEE conference on Consumer communications and networking conference IEEE Press Piscataway, NJ, USA. 2010

[14] Farbod Hosseyndoost Foomany, Alex Hirschfield, Michael Ingleby, "Toward a Dynamic Framework for Security Evaluation of Voice Verification Systems", International Conference on Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto.2009, pp 22-27

[15] Shan Kang, Naiwen Chen, Mi Yan, Xiaoxiao Chen, “Detecting Identity-Spoof Attack Based on BP Network in Cognitive Radio Network”.2011, pp 1603 – 1606

[16] Zahid Akhtar, Battista Biggio, Giorgio Fumera, and Gian Luca Marcialis, “Robustness of Multi-modal Biometric Systems under Realistic Spoof Attacks against All Traits”, IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS 2011), Milan, Italy. 2011 pp. 5-10ition Workshop. IEEE Odyssey. 2006 pp 1-8