International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 193– 195

Discrete Wavelet Transforms Algorithm Used for Automatic Signature Authentication

Ms.Prajakta Randive(M-tech IV Sem)
Computer Science and Engg.
Priyadarshini Institute of Engineering and Technology
Nagpur, India
Email:randive.pranjali@gmail.com

A.S. Sambare(Asst.Prof)
Computer Science and Engg.
Priyadarshini Institute of Engineering and Technology
Nagpur,India
Email:ashishsambare@hotmail.com

Abstract— In this paper, we propose automatic signature authentication system based on Discrete Wavelet Transform. Steps for verifying online handwritten signature in this system start with extracting pen position data (x and y positions) of points that forming the signature. Pen position data derived by Pen-movement angles.Data are normalized and resampled when to reduce variations in pen-position and pen-movement angles dimensionality. The signature is verified in DWT domain to enhance the difference between a genuine signature and its forgery. Intrapersonal features considered in low frequency sub-band signals (approximations) of pen-position parameter and pen-movement angle parameter. These are used for suppressing variations between different genuine signatures and enhancing the interpersonal variations, hence higher scores within total recognition process are given.Decision about online handwritten signature verification depend on both of pen-position and pen-movement angle features.

Keywords- *Online signature, mobile device authentication , Discrete Wavelet Transform, feature extraction ,verification*

*****

I. INTRODUCTION

Recently a significant amount of research is going on to ensure secure communication in wireless networks. The implementation of security schemes at physical layer becomes a hotspot, as the high-layer secure protocols have attracted growing attacks in recent years. Due to broadcast nature of wireless transmission, the transmitted messages are susceptible to be intercepted by eavesdroppers. However, due to the fading effect and the broadcast property of radio transmission, wireless communication are always vulnerable to eavesdropping which consequently makes security schemes of great importance in it as a promising approach to communicate confidential messages and so the secrecy capacity is severely limited in wireless communications. If the eavesdropper node is not detected within appropriate time then the messages transmitted in the network could be read and used for malicious activities. To that end, user cooperation as an emerging spatial diversity technique can effectively combat wireless fading and thus improves the secrecy capacity of wireless transmissions in the presence of eavesdropping attack. In particular, node cooperation via relays can increase the achievable secrecy rate by exploiting/mitigating the channel effects. There are mainly two relaying protocols for the cooperative secure transmission: decode and-forward (DF) and amplify-and-forward (AF). The secrecy rate based on single-antenna systems is hampered by channel conditions.

Cooperative communications uses multiple nodes which help each other to transmit messages and has been widely acknowledged as an effective way to improve system performance. Beamforming is an attempt to achieve spatial diversity through the use of the partner's antenna. Apart from the cellular scenario, user cooperation diversity has the potential to be successfully used in wireless ad hoc networks also. Typically, the main channel capacity with multiple relays can be significantly increased by using cooperative beam forming. More specifically, multiple relays can form a virtual antenna array and cooperate with each other to perform transmit beam forming such that the signals received at the intended destination experience constructive interference while the others (received at eavesdropper) experience destructive interference. With the cooperative beam forming, the received signal strength of destination will be much higher than that of eavesdropper. In DF relaying protocol the relay first decodes its received signal from source and then re-encodes and transmits its decoded outcome to the destination. In an AF protocol, the source broadcasts message in the form of signal in the first hop where the information symbol is selected from a codebook and is normalized. The received signal at relay is the actual message with additive noise. In the second hop, each relay forwards a weighted version of the noisy signal it just received. Amplify and forward relay networking scheme is simplest among them where each node transmits the message it has received after amplification (scaling). Though simplest in nature but the significance of this scheme lies in its low cost implementation and effectiveness against fading.

In this paper, we propose an auto regression technique and RC6 algorithm for maximizing the secrecy capacity of message being transmitted within a wireless relay network. For this, assuming that the global channel state information (CSI) is available, we consider a multi-hop network consisting of a single source and a single destination along with multiple relay nodes in between. However, due to the presence of one or more eavesdropper, secrecy of communication is in jeopardy. For such a scenario secrecy rate of the network provide a good measure of performance of the system. Unlike some previous works where only total relay power constraints are assumed, we consider the individual relay power constraint also. Generally, in practice, the relay nodes are powered by their

individual power source without any means to share their power sources (e.g. battery). Therefore, individual relay constraint is more relevant in practical situations and general.

Auto regression technique here takes power consumption constraint into consideration. The proposed system is considered to be an ergodic system which is based only on past or present values of each node within a wireless relay network that participates in data transmission. In order to gain high efficiency this strategy of auto regression can be very helpful since it deals with power consumption in this paper. At each moment while transmitting message or signal the sensor's power consumption output will be compared to an alredy set threshold value. If the threshold value exceeds, it can be easily possible to detect an eavesdropper node since it may consume more power in order to process or observe the data for its malicious use

The RC6 algorithm on the other hand provides a way to secure the transmission by encoding the message in such a way that if any other node except the trusted ones try to decode the message by applying a random incorrect key, then the message will be destroyed and will not be available again to that suspicious eavesdropper node. Now since the feedback is included in the network due to cooperative relays. The missing packet can be recognized and resent from a different route. In this way, the proposed paper provides a 2- way secure approach for achieving secrecy in confidential message transmission in wireless relay networks using beamforming..

II. Overview of Existing Methods

Most of the signature verification work done in the past years focused either on offline system or online system approaches.Automatic verification system of online handwritten signature to prevent identity fraud by verifying the authenticity of signatures on Australian passports is presented.
In previous system following survey are done:- In [1] proposed that Automatic handwritten signature verification system to prevent identity fraud by verifying the authenticity of signatures on Australian passports. An automatic handwritten signature verification and forgery detection system for authenticating signatures is presented . In [2] proposed that a new hybrid handwritten signature verification system where the on-line reference data acquired through a digitizing tablet serves as the basis for the segmentation process of the corresponding scanned data. Local foci of attention over the image are determined through a self-adjustable learning process in order to pinpoint the feature extraction process. In this paper processed by local and global primitives and the decision about the authenticity of the specimen is defined through similarity measurements. Measured global performance of the system using two different classifiers. In [3] proposed that a method for verifying handwritten signatures where various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen pressure, etc signature features are extracted and used to train the NN. Several Network topologies accuracy is compared and and Network topologies are tested. For the best case resulting system performs reasonably well with an overall error rate of 3:3% being reported.In [4] Handwritten signature verification system based on a Hidden Markov Model approach for representing and verifying the hand signature data. In [5] proposed that On-line signature verification the time functions of the dynamic signing process (e.g., position trajectories, or pressure versus time) are available for recognition. In [6] proposed that a simple and efficient method for online signature verification. The feature set of technique comprising of several histograms that can be computed efficiently given a raw data sequence of an online signature.Experimental results demonstrate that the performance of the proposed technique is comparable to state-of-art algorithms despite its simplicity and efficiency. In [9]proposed that The commonly used warping technique is dynamic time warping (DTW). It was originally used in speech recognition and has been applied in the field of signature verification with some success.Another new warping technique we propose is named as extreme points warping (EPW). It proves to be more adaptive in the field of signature verification than DTW.Through matching the EPs and warping the segments linearly, we achieve the goal of warping the whole signal.

III. Conclusion

In this paper, we proposed online signature verification system based on discrete wavelet transform.Some parameters of handwritten signature data were decomposed into sub-band signals by DWT. High frequency (details) sub band signals and Low frequency approximations) sub band signals were extracted for these parameters. The results show that success rate of the recognizer is 100% when tested with signatures it has been trained to recognize. When using all the extracted DWT approximation features, the success rate of the recognizer is up to 90% when tested with untrained genuine signatures.

References

[1] Madasu Vamsi K, Lovell Brian C, Kubik Kurt. Automatic handwritten signature verification system for australian passports. In: Science, engineering and technology summit on counterterrorism technology, Canberra, 14 July, 2005. p. 53–66

[2] Zimmer Alessandro, Ling Lee Luan. A hybrid on/off line handwritten signature verification system. In: Seventh international conference on document analysis and recognition (ICDAR'03), vol. 1; 2003. p. 424

[3] Trevathan Jarrod, Read Wayne, McCabe Alan. Neural network based handwritten signature verification. J Comput 2008;3(8): 9–22

[4] McCabe A, Trevathan J. Markov model-based handwritten signature verification. In: International conference on embedded and ubiquitous computing (IEEE/IFIP); 2008

[5] Tolba AS. GloveSignature: a virtual-reality-based system for dynamic signature verification. Digital Signal Process 1999;9(4): 241–66

[6] N. Sae-Bae and N. Memon, "A simple and effective method for online signature verification," in Proc. Int. Conf. BIOSIG, 2013, pp. 1–12.

[7] Bandyopadhyay SK, Bhattacharyya D, Das P. Handwritten signature recognition using departure of images from independence. In: 3rd IEEE conference on industrial electronics and applications (ICIEA 2008), Singapore, 2008

[8] Zimmer Alessandro, Ling Lee Luan. Offline signature verification system based on the online data. EURASIP J Adv Signal Process 2008;2008:Article No. 112

[9] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW,"*Pattern Recognit.*, vol. 40, no. 3, pp. 981–992, 2007

[10] Lee Luan L, Berger Toby, Aviczer Erez. Reliable on-line human signature verification systems. IEEE Trans Pattern Anal Mach Intell 1996;18(6):643–7

[11] Ong Thian Song, Khoh WH, Teoh A. Dynamic handwritten signature verification based on statistical quantization mechanism

[12] Nakanishi I, Sakamoto H, Nishiguchi N, Itoh Y, Fukui Y. Multimatcher on-line signature verification system in DWT domain.IEICE Trans Fundam 2006;E89-A(1):178–85

[13] Lejtman Dariusz Z, George Susan E. On-line handwritten signature verification using wavelets and back-propagation neural networks. In: Sixth international conference on document analysis and recognition (ICDAR'01); 2001. p. 0992

[14] Nanni Loris, Lumini Alessandra. A novel local on-line signature verification system. Elsevier; 2007.

[15] Faundez-Zanuy M, Sesa-Nogueras E, Roure-Alcobe J (2012) On the relevance of aging in handwritten biometric recognition. In: IEEE Int. Carnahan Conf. onSecurity Technology. 105–109.

.