Biomedical Research 2017; 28 (3): 1036-1039 *ISSN 0970-938X*
www.biomedres.info

An approach for detecting offline intrusive attacks on biomedical information.

Bala Krishnan R[1*], Raajan NR[2]

[1]Department of CSE, Srinivasa Ramanujan Centre, Sastra University, India

[2]School of EEE, SASTRA University, India

Abstract

The procedure of sharing the diagnostic medical reports and the scanned images of patients among doctors in a secured fashion with corresponding suggestions for joint treatment creates greatest care for the patients through quicker and crucial decisions. Intrusion Detection is the essential part of Information and Network Security domain in opposition against illegal access or malicious attacks. In this context, a new mechanism has been projected to detect offline Intrusion Detection System over the medical images. The proposed scheme deals with Image Blocks matching for the intrusive and normal pattern detection. From the experimental results, the proposed scheme detects the attacks namely: R2L, U2R and DoS. The observation shows that the proposed model offers high efficient detection and accuracy. This model gives realistic results over the Biomedical Images (Ex. DICOM).

Keywords: Intrusion detection system, Information security, Block detection, Anomaly detection, Pattern matching.

Accepted on July 7, 2016

Introduction

The growth of internet and its usage leads the modern communication technology era. Because of the tremendous growth of internet and its associated fields like Medicine, tele-consulting, Data Transmission and Information hiding, the need for securing the data and its confidentially gets improved. Hence the need of Intrusion Detection Systems (IDS) plays the crucial part of the cyber security systems at the information and network security areas over the field of Medical Diagnosis. IDS have drawn significant research attentions recently [1,2]. Principally, the IDS terminologies have been classed into two categories: Anomaly detection and misuse or signature-based detection [1,3]. Anomaly intrusion detection tries to identify the abnormal pattern by checking it with previously saved pattern; whereas the misuse detection identifies the intrusive attacks by known signatures. Now the procedure of inter communication between the organizations plays the lead role in business. Hence the need of IDS and Intrusion Prevention Systems (IPS) for the organizations is essential. IDS are a security mechanism that identifies the arrival of attacks to the sources and IPS terminates the attacks, which are identified by the IDS. Designing of IDS and IPS are majorly classified into two categories on the basis of their nature. The categories are: Online IDPS (Intrusion Detection and Prevention Systems) and Offline IDPS.

Online IDS deals with the network oriented intrusive attacks detection, whereas the Offline IDS works with the stored data and check for the availability of unknown or attack patterns and the data which it holds would be classed into two categories such as training and testing data.

For IDS applications the available standard data patterns are: DARPA, KDD99 and NSL KDD. The most popular dataset for the IDS related research is KDD 99 with 41 parameters. Most of existing IDS mechanisms works on the principle of classification techniques and most of the classification algorithms incorporated in IDS follows the base of naive Bayesian procedure [4], Support Vector Machine [5], Particle Swarm Optimization [6], Genetic Algorithms [7], Neural Networks [8,9] etc.,

The rest of the paper is presented as follows. Section 2 provides an overview of related works carried out in IDS with Medical domain with Image Pattern matching; Section 3 offers the proposed methodology. Experimental results are presented in Section 4 and conclusion is stated in Section 5.

Related Works

The standard IDS in implemented in various platforms such as: Medicine, tele-consulting, Telecommunication, Media, Firewall etc., by following various approaches like machine learning, biological information, statistical and data mining [10]. Bala Krishnan et al., [4] presented a method to find the efficient parameters for attacks detection in IDS by basic and advanced classification techniques. The authors Laheeb [11] deals with distributed time-delay based artificial neural network for IDS enhancements. In this modern era of Information technology, multimedia tools have been utilized to

perform secret sharing of e-medical data sheets of patients among the authorized doctors for their references and for consultation and clarification. At present, some secured telemedicine implementations have been on demand because the images with medical domain have been used in various studies. The standard DICOM image offers more quality and comfort than normal images for the recipients. The reason is that the DICOM standard holds the e-medical data, which has more responsibility in terms of indemnity policies. It can be saved by crypto and stego techniques like: digital signatures, watermarking and hash functions.

Proposed System

The proposed Image Block Matching is an efficient mechanism of image and video processing terminology and its simplified working strategy is stated in Figure 1.

Figure 1. *Image block matching scheme with inputs and outcomes.*

It works by identifying the similarity between the images or frames of the video. The proposed model implementation starts by subdividing the Medical DICOM image into a number of sub-blocks of pixels with preferred Block Size (height, width) and is stated in Figure 2. The proposed methodology has been initiated to avoid intrusive attacks over the Medical data of Patients and the communication could be performed between the doctors. The Biomedical data has been transmitted over the network channel by embedding it over the Medical image using Bishop Tour based LSB mechanism [10]. The data holds the information about the medical history of the patient, details about the current health status, medicines suggested, previous treatment details and so on.

The need for the privacy over the data is that the intruder can have a possibility to track the details of the patient and later can release the details. In order to improve the security of the information the Medical data has been embedded into the Medical images (DICOM). The block matching procedure over the images starts by moving a pixel block in the frame f over a search region block on the frame f+1 which is limited by the height and width parameter and is stated in Figure 3, the dissimilarity between the blocks can be computed as a Mean Square Error (MSE).

The proposed DICOM Image based block matching focuses on two features of the block matching strategy, the ability of the model to estimate the motion range between two DICOM image blocks and the ability to obtain the mean square errors between two images as stated in Figure 4. The terminology estimation states the ability to generalize from incomplete data.

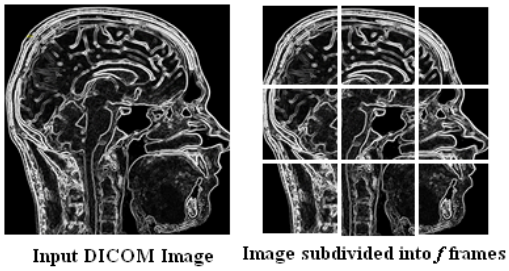

Figure 2. *Image sub blocks creation.*

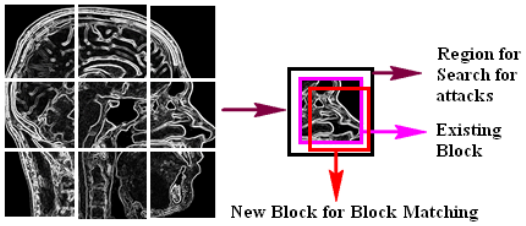

Figure 3. *Proposed image block comparison principle.*

The MSE states classified data as an attack signature or a normal request. There are two techniques to incorporate the DICOM Based image block matching technique on the IDS.

The first scheme is by creating testing data as a two dimensions matrix and pass it to sub-matrix block according to the size of the testing records, then it pass to the IDS Block detection mechanism as image under comparison with another DICOM image formed from training data, the obtained result will appear as matrix of MSE, this errors is passed to Embedded SCILAB5.4.1 version Function to obtain the decision if it is attack signature or a normal signature or not. If the DICOM image has been successfully classified as normal, then only the data extraction phase gets executed to obtain the secret medical data of the patient at the receiver end.

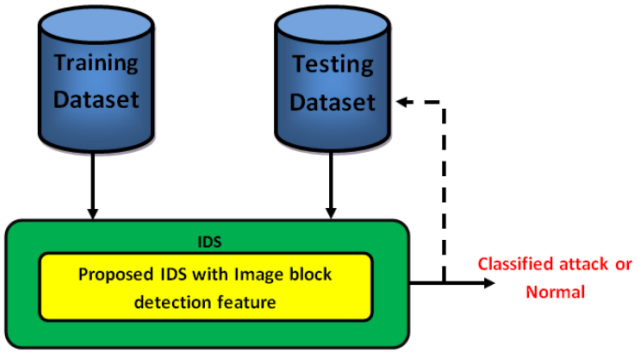

Figure 4. *Proposed ids execution phase.*

The second scheme is to generate a video clip from the multiple DICOM images of testing data and the patch data that is tacked from the training data then it passed to the IDS for the attack identification.

Experimental Observations

The proposed IDS have been implemented using SCILAB 5.4.1. The performance of the algorithm is assessed on a Pentium Core 2 Duo system of 2.6 GHz with 4 GB RAM on Windows 8 platform. The experiments have been conducted by considering the standard DICOM images with resolution 1024 × 1024 and the input images are shown in the Figure 5 and its corresponding Bishop Tour based stego images are shown in Figure 6.

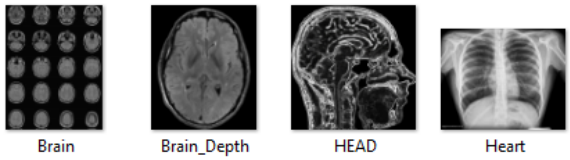

Figure 5. *Sample DICOM input images.*

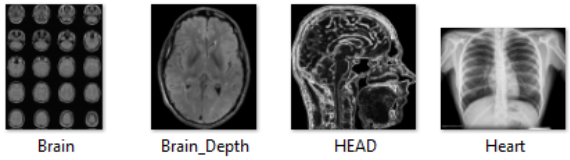

Figure 6. *Stego DICOM images.*

For the proposed IDS based testing, NSL KDD type dataset is taken for testing. Around 1800 testing patterns have been utilized for finding the three categories of attacks. The identified attacks are R2L, DoS and U2R. Where F_i is the number of features taken for the classification, n is the number of training dataset, *lbl* is the number of labels and tot is the total iterations. The Time Complexity for the proposed IDS to identify the three categories of attacks and its complexity measures are stated in the Table 1.

Table 1. *Attacks type and its time complexity.*

Attack type	Time complexity
DoS	*O ((F2-F1) lbl^2 n tot)*
U2R	*O ((F3-F2) lbl^2 n tot)*
R2L	*O ((F4-F3) lbl^2 n tot)*
Overall complexity	*O (F4 lbl^2 n tot)*

The training dataset contains 600 patterns on each category. The observed results are classed as Efficient Classifications (EC) and it could be computed in terms of percentage on test dataset.

$$EC = \frac{\text{Correct Instance}}{\text{Total Training Dataset Count}} \rightarrow (1)$$

From the experiments we obtained the EC value for all the categories of attacks and are stated in Table 2.

Table 2. *Efficient classifications of attacks on proposed IDS.*

S. No	Attack	Percentage
1	R2L	97.66
2	DoS	98.97
3	U2R	94.28

The average value of the attacks detection accuracy is 96.97 per cent. The observations from the proposed model are compared with some of the existing models and the results are stated in the Table 3. The quality of the stego image can be determined through the parameters: Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR).

MSE is to identify the squares of the error between two images. Usually it is a set of numerical values and its computing equation is

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\text{Image(i,j)} - \text{SImage(i,j)})^2$$

$$\rightarrow (2)$$

Table 3. *Accuracy comparatives of various IDS.*

Author	Classifier mechanism	Data set	EC observations			
			R2L	DoS	U2R	Avg
Abdullah [3]	IBM	NSL-KDD	93.8	96.3	94.6	94.9
Laheeb [11]	DTDNN	KDD-99	95.8	97.6	96.2	96.53
Vaitsek-hovich [2]	MLP and RNN	KDD-99	85.59	94.2	86.54	88.77
Proposed	DICOM Image Block Based Detection	NSL-KDD	97.66	98.97	94.28	96.97

Where image and s-image represents the input and stego image respectively and N^2 denotes the resolution value of images. The ratio between signal variance and reconstruction error variance is computed through the PSNR value and it can be computed through the following equation.

$$PSNR = 10\log_{10}\frac{255^2}{\text{MSE}} \rightarrow (3)$$

The following Table 4 shows the comparison outcomes of the Input and stego images.

Table 4. *Comparison of input and stego images.*

Input image	Stego image	PSNR	MSE
Brain	Brain	51.194	0.4940
Brain_depth	Brain_depth	56.384	0.1495
Head	Head	55.688	0.1755
Heart	Heart	56.991	0.13

The MSE value states that the variation between the images is very low and the similarity between the images are at the acceptable rate, which are observed through the PSNR value.

Conclusion

In this paper a new mechanism is presented to share secured medical information about the patients between the doctors. This would be helpful for the medical data transmissions along with the medical images. The proposed model supports for the data transmission through the steganographic principles. The hidden data could not be viewed by the intruders and at the same time the prescribed medical history and suggestions for the treatment and requested suggestions between the doctors should be transmitted in a secured manner. The pattern of attacks detection could be performed in an efficient way and the proposed model offers an efficient classification rate for the attacks. From our experimental observations it is witnessed that the proposed model with DICOM images increase the strength of the ids application and the process of attacks detection on DICOM images would be simple and effective which helps to detect the attacks and normal data and safeguard the confidential data over the images. The process of detecting intrusive attacks over the videos would the future direction of this research work.

References

1. Shahbaa, Karma M. Network intrusion detection based on hybrid intelligence System. AL-Rafidain J Comp Sci Math 2012; 9: 81-98.
2. Abdullah AM. Designing of intrusion detection system based on image block matching. Int J Comp Comm Eng 2013; 2.
3. Vaitsekhovich L. Intrusion detection in TCP/IP networks using immune systems paradigm and neural network detectors. Brest St Tech Uni Int Owd 2009.
4. Bala Krishnan R. Efficient attributes identification practice on intrusion detection system dataset through prediction mechanisms. Far East J Electr Comm 2016; 2: 133-139.
5. Mukkamala S. Intrusion detection using neural networks and support vector machine. IEEE Int Honolulu 2002.
6. Guangyou Y. A modified particle swarm optimizer algorithm. Electr Meas Instr 2007; 2: 675-679.
7. Shazzad K, Park J. Optimization of intrusion detection through fast hybrid feature selection. Int Arab J Inf Technol 2014.
8. Golovko V, Kochurko P. Intrusion recognition using neural networks, in proceedings of intelligent data acquisition and advanced computing systems: technology and applications. Idassc 2005; 2005: 108-111.
9. Hofmann A, Schmitz C, Sick B. Rule extraction from neural networks for intrusion detection in computer networks. Man Cybern 2003; 1259-1265.
10. Bala Krishnan R. An enhanced biometric based intrusion detection system for secure communication. Far East J Electr Comm 2016; 1: 121-131.
11. Laheeb M. Anomaly network intrusion detection system based on distributed time-delay neural network. J Eng Sci Technol 2010; 5: 457-471.

*Correspondence to

Bala Krishnan R

Department of Computer Science and Engineering

Srinivasa Ramanujan Centre

Sastra University

India