ISSN: 2321-7782 (Online)
Volume 2, Issue 5, May 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Intrusion detection system using Expert system (AI) and Pattern recognition (MFCC and improved VQA)

Archit Kumar[1]
B.E , M.Tech , MBA
Dept of CSE , CBS Group
Haryana-India

Charu Chhabra[2]
B.tech , Msc,M.Tech(Pursuing)
Dept of CSE , CBS Group
Haryana-India

Abstract: ***This Paper presents the review of Intrusion Detection system using techniques of Expert systems (Artificial Intelligence).With the growing need of computer networking and e-commerce, the security of the web systems are of the major concern . IDS is the one that can be used for monitoring data congestion and also recognizing the user behavior to identify the malicious attacks and also the illegitimate access of intruders..The main aim of IDS is to safeguard the data confidentiality and integrity. Using the AI techniques once the intrusion is detected it can be represented using alerts to the security officer. The term to develops for intrusion detection in relation to border protection, perimeter detection, and similar guarding Home security, banking locker etc. The solutions provide early detection and warning by creating an extended virtual perimeter, thereby increasing the time available to react and ensuring that the correct measures are taken before disaster strikes. The recent MOtion-based Video Integrity Evaluation (MOVIE) index emerges as the leading objective VQA algorithm in our study, while the performance of the Video Quality Metric (VQM) and the Multi-Scale Structural SIMilarity (MS-SSIM) index is noteworthy. The LIVE Video Quality Database is freely available for download 1 and we hope that our study provides researchers with a valuable tool to benchmark and improve the performance of objective VQA algorithms. Mel Frequency Cepstral Coefficents (MFCCs) are a feature widely used in automatic speech and speaker recognition. They were introduced by Davis and Mermelstein in the 1980's, and have been state-of-the-art ever since. Prior to the introduction of MFCCs, Linear Prediction Coefficients (LPCs) and Linear Prediction Cepstral Coefficients (LPCCs) and were the main feature type for automatic speech recognition (ASR). This page will go over the main aspects of MFCCs, why they make a good feature for ASR, and how to implement them . An IDS examines the inbound and outbound activity of the network and also reports if any suspicious pattern is observed.***

Keywords: ***Intrusion Detection system, ANN, Expert system, Audio/ Video Processing, Neural Networks, MFCC, VQA algorithm, False Alarm, MOVIE, FFT.***

I. INTRODUCTION

First is the employment of intelligent image processing algorithms for facilitating the work of system operators. This leads to the second issue, related to improving social acceptance of surveillance systems, which can be achieved by limiting the amount of stored recordings only to the most relevant ones, in terms of security issues. Both of these matters are closely related, since the decision about certain video segments of being relevant or non-relevant can be made based on the implemented algorithms. This document is devoted to the description of several security related solutions. In the first section, existing complete commercial systems as well as smart camera devices are presented. All the indexed system solutions are compared in terms of the offered features and the characteristics of system architecture. This description is followed by an overview of existing smart surveillance cameras which are based on state of the art algorithms for automated intelligent video processing.

A description of projects related to video surveillance and security matters in general, is presented. Currently ongoing as well as already finished research projects are mentioned. Due to the growth of network environment complexity, the necessity of packet payload inspection at application layer is increased. String matching, which is critical to network intrusions detection systems, inspects payloads and detects malicious network attacks using a set of rules. In this paper we classify the sounds originated from humans, birds and cars. The motivation of such a classification is to detect the intruders into protected wildlife regions such as protected forests, lakes, and other natural reservations.

II. CATEGORIES OF IDS

The IDS have been classified into three main categories and they are Misuse detection Vs anomaly detection , Network based vs host based detection and passive vs reactive systems .

1. Misuse vs anomaly detection

The misuse detection part analyzes the information it gathers , and further it compares it to large databases of attack signatures by looking for a specific attack that has been documented . The anomaly detection on the other hand, compares the network segments to the normal parameters set by the administrator [1].

2. Network based vs Host based systems

In the network based systems, the network analyses individual packets of information flowing through it and detects if those are malicious. Whereas, in host based systems, the IDS examines network activities from each host computer [1]

3. Passive vs reactive systems

In passive systems, the IDS detect the security attack, notify with an alert and interrupt an alert signal whereas in the reactive systems performs the reaction by logging off the user and block the system from suspected malicious source.

III. DETECTION OF AN INTRUSION

The main goal of an IDS is to classify the intrusion based and nonintrusive network activities in a network segment in an effective manner. The process of Detecting an intrusion involves a series of steps for instance firstly, the collection of data is done , secondly Preprocessing of data is exhibited. Followed by the classification of the data and finally the computation of the result .To detect the intrusion our prime aim is to make the system understand what is an intrusion and also the methodology by the virtue of which it can interpret whether what are the different patterns or user behavior.

IV. AI TECHNIQUES

Artificial intelligence is not just a single name, rather it incorporates inter disciplinary endeavors within it. AI comprises of concepts like Neural networks , Artificial neural networks , fuzzy logic , support vector machines and even includes pattern recognition, Image analysis and Operation analysis which can be perfectly implemented while detecting the intrusion in a network based system. In real world, IDS requires processing of high dimensions of network system. The incorrect alarming of the IDS can be a cause of alarms that were triggered by benign events .therefore we can say that traditional IDS generates maximum probability of generating false alarms. One way to overcome this situation is to achieve such implementation so that the IDS are constructed in such a way that they produce fewer false alarms. The most important point of concern is to reduce the count of false alarms as it may lead to the occurrence of certain more problems. There are a number if AI based techniques used for classifying the data patterns and also implementing in a way that minimum possible false alarms are observed. Hence such AI techniques includes Neural networks techniques , Decision based techniques , rule based techniques , data mining techniques , genetic algorithm based techniques , pattern recognition techniques and so forth. If we discuss about the requirement of AI based IDS when compared to traditional IDS, we can observe from the background work that traditional IDS used to work in such a manner that the system administrator used to add new rules for every new type of attack. But in AI Based IDS there are

no such requirements. The AI based IDS can learn and implement new rules effectively without troubling the system administrator much.

V. CONNECTION OF ANN AND IMAGE PROCESSING

Classifying the user behavior or the system behavior is very difficult in IDS. At some instance of time it becomes very difficult to classify the behavior patterns of the normal user and the intruder. Artificial intelligence and the concept of artificial neural networks inculcate the potential of resolving number of problems as compared to the traditional IDS.

A neural network is the collection of simple units called neuraons. In computer science, the ANN is computational models that are inspired by the central nervous system, the brain. ANN is capable of machine learning and Pattern recognition (Image processing) which can be heavily useful in detecting the intrusion. The most important functional feature of ANN is its capacity to learn. Traditional IDS used to have a fixed pattern of learning which was prepared in advanced. They used to work with a turing like machine in which the output is always static and new pattern and rules cannot be adapted which performing . the first model of ANN was introduced by McCulloch and Pitts in the year 1943. The implementation of ANN in real engineering and scientific progress was done by Rosenblatt in the year 1958 by developing the Perceptrons.

The concept of perceptrons is very useful in Pattern recognition and classification which can be beneficial in classifying and determining the user behavior and clustering the intruder accordingly. Artificial Neural networks find their application in Pattern recognition (Clustering, classification and feature selection).

IDS can be exploited as a Pattern recognition technique. Pattern recognition can be implemented by using a feed – forward neural network .

The handshaking of ANN and Pattern recognition can thereby detect the behavioral pattern of the intruder and can follow with the actions reporting the occurrence of intrusion detection.

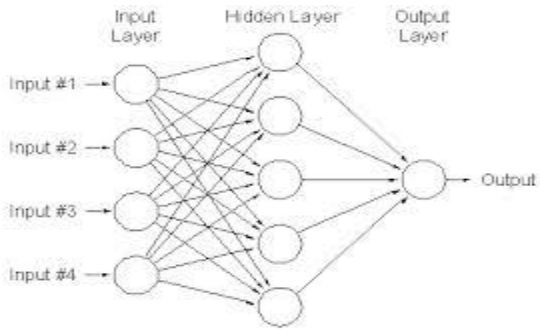


Figure: Artificial neural network

VI. TRAINING AND LEARNING ARCHITECTURE IN NEURAL NETWORK

Neural networks can be divided into two categories: static and dynamic architecture. In the static or feed forward networks have no elements for feedback. The output calculation in the feed forward networks is done only by the input provided to them. In contrast to static architecture, the dynamic architecture works in such a manner that the output depends on the current inputs and also previous inputs.

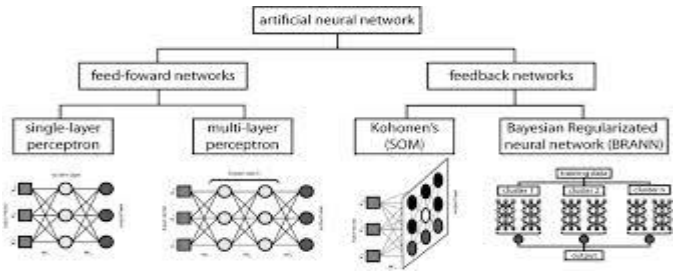


Figure: Categories of ANN

VII. Supervised and Unsupervised Learning in ANN

Feed forward neural networks are the simplest neural networks [3] . The further implementation of the feed forward networks is the multilayer feed forward networks which may include backpropagation algorithms . The other category is the Recurrent networks . The recurrent networks are used when there is major deviation between the predicted output and the measured one . Once such a major deviation in the form of intrusion is observed , alarm is issued depicting the presence of different behavioral pattern . part of such learning . SOMs are used in Intrusion detection by clustering the similar objects in one cluster and different patterns as outliers . Moradi and Zulkernine used the multilayer perceptrons based neural networks with good results . A Multilayer perceptron consists of an input layer , one or several hidden layers ,and an output layer . The main objective of MLPs is to classify different types of attacks.Unsupervised learning is the one which resembles the concept of statistically clustering theory . In the same the clustering is done by grouping the objects that are similar in nature . Self Organizing Maps abbreviated as SOMs are used in Intrusion detection by clustering the similar objects in one cluster and different patterns as outliers . Moradi and Zulkernine used the multilayer perceptrons based neural networks with good results . A Multilayer perceptron consists of an input layer , one or several hidden layers ,and an output layer . The main objective of MLPs is to classify different types of attacks.

VIII. Performance of VQA Algorithms

The performance of several publicly available objective VQA models was evaluated on our database. Many popular VQA algorithms are licensed and sold for profit and are not freely available. We tested the following VQA algorithms on the LIVE Video Quality Database.

- Peak Signal to Noise Ratio (PSNR) is a simple function of the Mean Squared Error (MSE) between the reference and test videos and provides a baseline for objective VQA algorithm performance.

- Structural SIMilarity (SSIM) is a popular method for quality assessment of still images that was extended to video.The SSIM index was applied frame-by-frame on the luminance component of the video and the overall SSIM index for the video was computed as the average of the frame level quality scores. Matlab and Labview implementations of SSIM are freely available for download.

- Multi-scale SSIM (MS-SSIM) is an extension of the SSIM paradigm, also proposed for still images that has been shown to outperform the SSIM index and many other still image quality assessment algorithms.We extended the MS-SSIM index to video by applying it frame-by-frame on the luminance component of the video and the overall MS-SSIM index for the video was computed as the average of the frame level quality scores. A Matlab implementation of MS-SSIM is freely available for download.

- Speed SSIM is the name we give to the VQA model that uses the SSIM index in conjunction with statistical models of visual speed perception. Using models of visual speed perception was shown to improve the performance of both PSNR and SSIM. We evaluated the performance of this framework with the SSIM index, which was shown to perform better than using the same framework with PSNR.

A software implementation of this index was obtained from the authors.

- Visual Signal to Noise Ratio (VSNR) is a quality assessment algorithm proposed for still images and is freely available for download. We applied VSNR frame-by-frame on the luminance component of the video and the overall VSNR index for the video was computed as the average of the frame level VSNR scores.

- Video Quality Metric (VQM) is a VQA algorithm developed at the National Telecommunications and Information Administration (NTIA).24 Due to its excellent performance in the VQEG Phase 2 validation tests, the VQM methods were adopted by the American National Standards Institute (ANSI) as a national standard, and as International Telecommunications

Union Recommendations (ITU-T J.144 and ITU-R BT.1683, both adopted in 2004). VQM is freely available for download for research purposes.

- V-VIF is the name we give to the VQA model that extends the Visual Information Fidelity (VIF) criterion for still images to video using temporal derivatives. A software implementation of this index was obtained from the authors.

- MOtion-based Video Integrity Evaluation (MOVIE) index is a VQA index that was recently developed at LIVE. Three different versions of the MOVIE index - the Spatial MOVIE

IX. MFCC ALGORITHM FOR AUDIO PROCESSING

Step1. Frame the signal into short frames.

Step2. For each frame calculate the periodogram estimate of the power spectrum.

Step3. Apply the mel filterbank to the power spectra, sum the energyin each filter.

Step4. Take the logarithm of all filterbank energies.

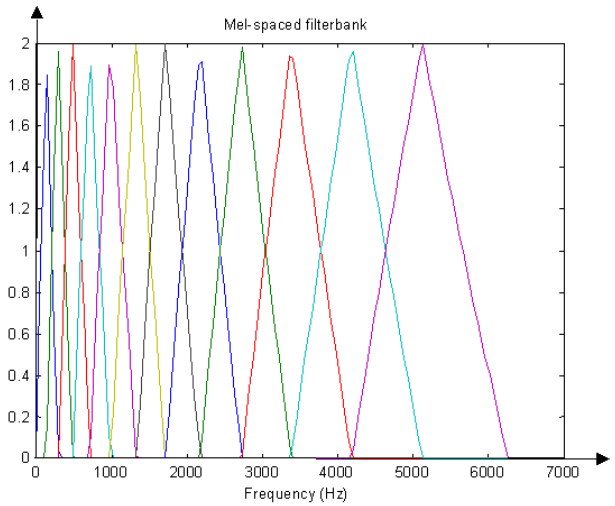
Step5. Take the DCT of the log filterbank energies.

Step6. Keep DCT coefficients 2-13, discard the rest.

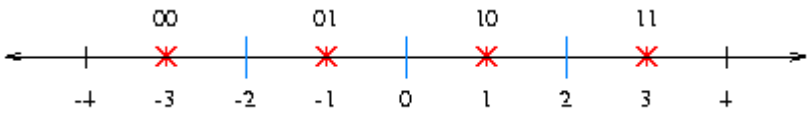
X. METHODOLOGY

[a] Intrusion detection using audio processing

The Mel scale relates perceived frequency, or pitch, of a pure tone to its actual measured frequency. Humans are much better at discerning small changes in pitch at low frequencies than they are at high frequencies. Incorporating this scale makes our features match more closely what humans hear.



A VQ is nothing more than an approximator. The idea is similar to that of ``rounding-off" (say to the nearest integer). An example of a 1-dimensional VQ is shown below:



Here, every number less than -2 are approximated by -3. Every number between -2 and 0 are approximated by -1. Every number between 0 and 2 are approximated by +1. Every number greater than 2 are approximated by +3. Note that the approximate values are uniquely represented by 2 bits. This is a 1-dimensional, 2-bit VQ. It has a rate of 2 bits/dimension.

The formula for converting from frequency to Mel scale is:

$$M(f) = 1125 \ln(1 + f/700) \qquad (1)$$

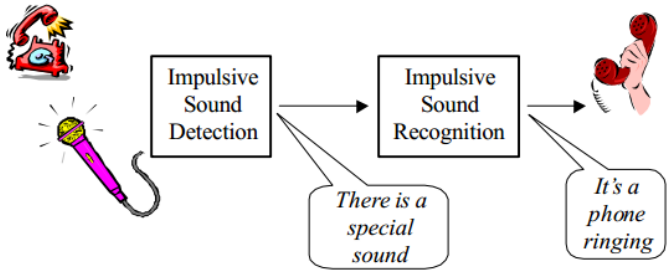
To go from Mels back to frequency:

$$M^{-1}(m) = 700(\exp(m/1125) - 1) \qquad (2)$$

That there are 16 regions and 16 red stars -- each of which can be uniquely represented by 4 bits. Thus, this is a 2-dimensional, 4-bit VQ. Its rate is also 2 bits/dimension.

In the above two examples, the red stars are called code vectors and the regions defined by the blue borders are called encoding regions. The set of all code vectors is called the codebook and the set of all encoding regions is called the partition of the space.

To get the filter banks shown in figure 1(a) we first have to choose a lower and upper frequency. Good values are 300Hz for the lower and 8000Hz for the upper frequency. Of course if the speech is sampled at 8000Hz our upper frequency is limited to 4000Hz. Then follow these steps:



Using equation 1, convert the upper and lower frequencies to Mels. In our case 300Hz is 401.25 Mels and 8000Hz is 2834.99 Mels.

For this example we will do 10 filterbanks, for which we need 12 points. This means we need 10 additional points spaced linearly between 401.25 and 2834.99. This comes out to:

m(i) = 401.25, 622.50, 843.75, 1065.00, 1286.25, 1507.50, 1728.74,

1949.99, 2171.24, 2392.49, 2613.74, 2834.99

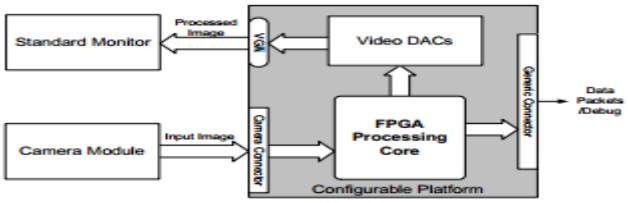
Now use equation 2 to convert these back to Hertz:

f(i) = 300, 517.33, 781.90, 1103.97, 1496.04, 1973.32, 2554.33,

3261.62, 4122.63, 5170.76, 6446.70, 8000. Notice that our start- and end-points are at the frequencies we wanted.

6. Now we create our filterbanks. The first filterbank will start at the first point, reach its peak at the second point, then return to zero at the 3rd point. The second filterbank will start at the 2nd point, reach its max at the 3rd, then be zero at the 4th etc.

[b] Intrusion Detection Using Video Processing



XI. CONCLUSION

Intrusion detection of obstacle is an important issue as it can save a significant part of the breeder's work hours. From the experiments, we found that automatic detection of obstacle using sound and video processing activty data can be an efficient and economical solution. A combination of MFCC with feature dimension reduction and VQA can automatically intruder at an accuracy level of over 94%. As the sound data acquired from even a cheap microphone can detect human accurately and economically, our method can be used either as a standalone solution or to complement other known methods to obtain a more accurate solution. Moreover, this study might be a confirmation that video and sound understanding of cow calls is an amendable method to understand the animal's present conditions. For future work, we will consider the multi-modality of the video and audio data. Further testing and refinement of our proposed system, as needed, in commercial production settings are also warranted. That is, a complete real-time system, capable of incorporating the automatic recognition, is a part of ongoing our research

References

1. Sans institute infosec reading room, Understanding Intrusion Detection System, Internet, sans institude ,1 to 9, 2001.

2. Karen Scarfone, Peter Mell, Guide to Intrusion detection and prevention systems (IDPS), NIST, 1 to 127, 2007.

3. Tiwari Nitin, S. R. Singh and P. G. Singh, Intrusion Detection and Prevention System (IDPS) Technology- Network Behavior Analysis System (NBAS), International Science Congress Association , 51-56, July (2012).

4. B. Raju1 and B. SrinivasNetwork Intrusion Detection System Using KMP Pattern Matching Algorithm, IJCST,33-36, January 2012

5. C. U. Chauhan and V.A.Gulhane, Signature Based Rule Matching Technique in Network Intrusion Detection System, internet, 412-416, April 2012.

6. Faisal Mahmood , INTRUSION DEECTION SYSTEM using Sax 2.0 and wireshark 1.2.2, Internet, 1-19, 10/6/2009

7. Davis, S. Mermelstein, P. (1980) Comparison of Parametric Representations for Monosyllabic Word Recognition in Continuously Spoken Sentences. In IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 28 No. 4, pp. 357-366

8. X. Huang, A. Acero, and H. Hon. Spoken Language Processing: A guide to theory, algorithm, and system development. Prentice Hall, 2001.

9. H. Hermansky, "Perceptual linear predictive (PLP) analysis of speech", J. Acoust. Soc. Am., vol. 87, no. 4, pp. 1738-1752, Apr. 1990.

10. H. Hermansky and N. Morgan, "RASTA processing of speech", IEEE Trans. on Speech and Audio Proc., vol. 2, no. 4, pp. 578-589, Oct. 1994.

11. Mitchell, R. S., R. A. Sherlock, and L. A. Smith. 1996. An investigation into the use of machine learning for determining oestrus in cows. Comput. Electron. Agric. 15:195-213.

12. Nebel, R. L., M. G. Dransfield, S. M. Jobst, and J. H. Bame 2000. Automated electronic systems for the detection of oestrus and timing of AI in cattle. Anim. Reprod. Sci. 60-61:713-723.

13. Peipei, S., C. Zhou, and C. Xiong. 2011. Automatic speech emotion recognition using support vector machine. International Conference on Electronic & Mechanical Engineering and Information Technology. 621-625.

14. Roelofs, J. B., F. J. Van Eerdenburg, N. H. Soede, and B. Kemp. 2005. Pedometer readings for estrous detection and as predictor for time of ovulation in dairy cattle. Theriogenology 64:1690-1703.

15. Ruiz-Garcia, L., L. Lunadei, P. Barreiro, and J. Robla. 2009. A review of wireless sensor technologies and applications in agriculture and food industry: state-of-the-art and current trends. Sensors 9:4728-4750.

16. Saint-Dizier, M., and S. Chastant-Maillard. 2012. Towards an automated detection of oestrus in dairy cattle. Reprod. Domest. Anim. 47:1056-1061 doi: 10.1111/j.1439-0531.2011.01971.x.

