International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 277 - 283, 2014, ISSN: 2319–8656

Moving Object Detection with Fixed Camera and Moving Camera for Automated Video Analysis

Dipali Shahare
Department of Computer Science and Engineering,
G.H.Raisoni Institute of Engineering and Technology for women's, Nagpur, India.

Ranjana Shende
Department of Computer Science and Engineering,
G.H.Raisoni Institute of Engineering and Technology for women's, Nagpur, India

***Abstract*—** Detection of moving objects in a video sequence is a difficult task and robust moving object detection in video frames for video surveillance applications is a challenging problem. Object detection is a fundamental step for automated video analysis in many vision applications. Object detection in a video is usually performed by object detectors or background subtraction techniques. Frequently, an object detector requires manual labeling, while background subtraction needs a training sequence. To automate the analysis, object detection without a separate training phase becomes a critical task. This paper presents a survey of various techniques related to moving object detection and discussed the optimization process that can lead to improved object detection and the speed of formulating the low rank model for detected object.

***Index Terms*—** Object Detection, Soft Impute method, Markov Random Field, Temporal Differencing, Moving object extraction, background subtraction.

1.INTRODUCTION

Automated video analysis is important for many vision applications [11]. There are three key steps for automated video analysis: object detection, object tracking, and behavior recognition. As the first step, object detection aims to locate and segment interesting objects in a video. Then, such objects can be tracked from frame to frame, and the tracks can be analyzed to recognize object behavior. Thus, object detection plays a critical role in practical applications.

The primary goal of this paper is to critically discuss the various techniques for detecting moving objects methods in static and dynamic background in video. A second goal is to present a technique for formulating low rank model for detected object.

The rest of the paper is organized as follows: section 2 we discuss existing approaches for Moving Object Detection techniques, while section 3 discuss the proposed method for detecting object accurately and section 4 is summarized in the conclusions.

I. MOVING OBJECT DETECTION TECHNIQUE

Detection and extraction of moving object form a video sequences is used in various application like Video surveillance system, Traffic monitoring , Human motion capture, Situational awareness, Border protection and monitoring ,Airport safety.

Moving object can be detected from video sequences of either a fixed or a moving camera.

The main purpose of foreground detection is to distinguishing foreground objects from the stationary background. Detection of moving objects in video images is very important. The automatic detection of moving objects in monitoring system needs efficient algorithms. The common method is simple background subtraction i.e to subtract current image from background. But it can't detect the difference when brightness difference between moving objects and background is small. The other approach is to use some algorithms such as color based subtraction technique.

There are several methods to detect moving objects, which are given below:

A. Optical Flow Method

Optical flow method is a complex and bad anti-noise performance, and it cannot be applied to real-time processing without special hardware device. [14] Proposes an automatic extraction technique of moving objects using x-means clustering. In this proposed method, the feature points are extracted from a current frame, and x-means clustering classifies the feature points based on their estimated affine motion parameters. A label is assigned to

the segmented region, which is obtained by morphological watershed, by voting for the feature point cluster in each region. The labeling result represents the moving object extraction.

B. Consecutive Frames Subtraction

Consecutive Frames Subtraction is a simple operation, realizes easily and has strong adaptability on the dynamic changes in the environment. But it cannot be completely extracted moving targets. [15] proposes a novel method for extracting moving objects from video sequences, which is based on Gaussian mixture model and watershed, is proposed where first the difference between neighboring frames is calculated and is described by a Gaussian mixture model, then divided into moving areas and background by improved Expectation-Maximization (EM) algorithm.

C. Background Subtraction

Background subtraction is a common method for detecting moving objects and it has been widely used in many surveillance systems, but it is yet a difficult problem to distinguish moving objects from backgrounds when these backgrounds change significantly. Separating foreground from background in a video sequence is one of the most fundamental tasks in many applications of computer vision. To detect moving objects, each incoming frame is compared with the background model learned from the previous frames to divide the scene into foreground and background. Therefore, background modeling has been actively investigated in the past decade. The difficulty encountered in background modeling is that the outdoor backgrounds are usually non-stationary in practice. Broadly speaking, there are two categories of online methods to model the background. The first one models the background using a single model per pixel, whereas the second one employs multiple models per pixel. Background subtraction is a widely used approach for detecting moving objects from static cameras [16].

The four major steps in a background subtraction Algorithm are:

- Preprocessing
- Background Modeling
- Foreground Detection
- Data validation

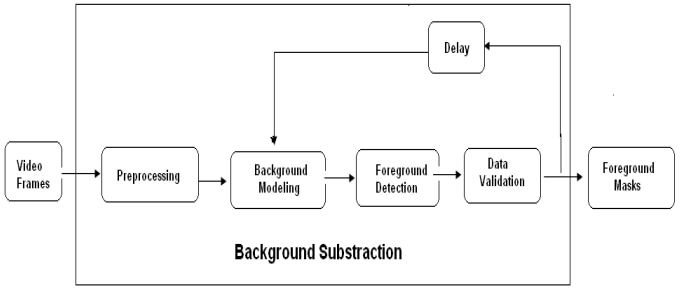


Figure 1.Illustration of Background Subtraction

In background subtraction, the general assumption is that a background model can be obtained from a training sequence that does not contain foreground objects.

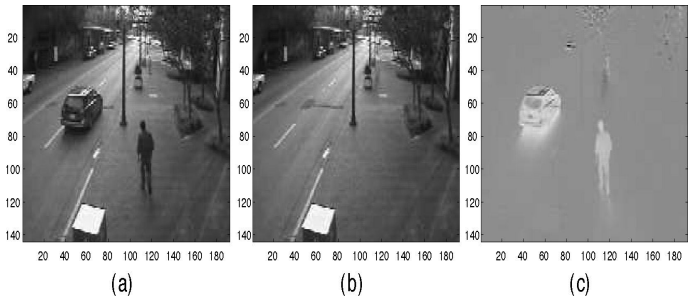


Figure 2. Decomposition-based background subtraction: (a) an input image with objects, (b) reconstructed image after projecting input image onto the, (c) difference image.

Color and Edge Information:

Jabri, et al. [4] proposed an approach in which background modeling and subtraction approach are used to detect a human in the video images. This approach is used to segment the person from the background by computing the mean image for all video sequences. The incoming frame is subtracted from the mean image to identify the pixels which have changed the color. However, the problem with this approach is both the color and edge channel are subtracted separately before finding the result and, as a consequence, the computational time increases.

Standard Subtraction:

The method developed by Davis and Taylor [5] is a motion-based method for differentiating normal walking movements at multiple speeds when atypical or non walking locomotion is involved. Human walking movements are detected using low level regularities and constraints. The person's shape in each video frame is extracted with standard background subtraction. This approach locates the head, waist and feet using the W4 approach [6]. Standard subtraction techniques, which use RGB pixel differences, dilations and removal of small pixel region, are employed. The centroid of the outline pixel is called the head pixel, while the mean value of silhouette pixels in the torso region is called the waistline. The waistline is divided into two halves in order to locate information relating to the

feet. Dynamic regularity features are calculated using cycle time, stance/swing ratio and double support time. Dynamic regularity features are independent of the camera position, but this approach uses view-based constraint of extension angle, which is suitable for non-walking locomotion and not for other regular locomotion's.

Object Extraction:

The algorithm proposed by Yoginee, et al. [13] has moving object segmentation, blob analysis and tracking. Blob analysis is used to count the vehicle from which the speed and flow are calculated. Boundary Block Detection (BBD) algorithm is used for moving object detection by identifying the blocks which contain the moving objects boundaries. The system requires the model background with no moving objects and scene which contain moving objects. The system finds the boundary of the moving objects and the number of moving objects from a given video scene. Aviread function [13], is used to extract all frames in the video. Background subtraction extracts the object, while the pixels of the background model image are used as threshold. All images are divided into two parts, viz., background and foreground in binarization. The new video frame was subtracted from those background images, if the pixel difference is higher than the threshold, that images are foreground or object. If the pixel significantly differs from the background image, then the pixel is marked as a moving object. Each image frame must update the threshold level. To count the moving object flow, the algorithm tracks each vehicle within successive image frames. This algorithm works only for the videos obtained from fixed cameras and which has the normal background and stable videos. The algorithm can be modified to work on complex background and videos that are not stable. In addition, the performance can be improved by using optimizing algorithm such as fuzzy logic and neural network.

Gaussian Mixture:

A Gaussian Model calculates each pixel-value from all the sample pixels' mean and variance. The model will set a lower bound and an upper bound that will eliminate pixels that are outside of the norm. If a video is to run for an extended period of time, the pixels' average will equal to the background's value unless the foreground object stays static. This is a common method for real-time segmentation of moving regions in frame sequences. Model Gaussians are updated using K-means approximation method. Each pixel is then evaluated and classified as a moving region or as a background.
Stauffer and Grimson [3] presented a novel adaptive online background mixture model that can robustly deal with lighting changes, repetitive motions, clutter, introducing or removing objects from the scene and slowly moving objects. Their motivation was that a unimodal background model could not handle image acquisition noise, light change and multiple surfaces for a particular pixel at the same time. Thus, they used a mixture of Gaussian distributions to represent each pixel in the model.

Temporal Differencing:

Temporal differencing method uses the pixel-wise difference between two or three consecutive frames in video imagery to extract moving regions. It is a highly adaptive approach to dynamic scene changes however, it fails to extract all relevant pixels of a foreground object especially when the object has uniform texture or moves slowly. When a foreground object stops moving, temporal differencing method fails in detecting a change between consecutive frames and loses the object.

Let Frame i represent the gray-level intensity value at pixel position i and at time instance n of video image sequence I, which is in the range [0, 255]. T is the threshold initially set to a pre-determined value. Lipton developed two frame temporal differencing scheme suggests that a pixel is moving if it satisfies the following:

$$| \text{Frame } i - \text{Frame } i\text{-}1| > th$$

This estimated background is just the previous frame. It evidently works only in particular condition of objects speed and frame rate and very sensitive to the threshold.

This method is computationally less complex and adaptive to dynamic changes in the video frames. In temporal difference technique, extraction of moving pixel is simple and fast. Temporal difference may left holes in foreground objects, and is more sensitive to the threshold value when determining the changes within difference of consecutive video frames [2]. Temporal difference require special supportive algorithm to detect stopped objects.

Comparison of several popular methods for moving object detection:

Optical Flow method	**Consecutive Frames Subtraction**	**Background Subtraction**
Complex and bad anti-noise performance	simple operation, realizes easily	provides a moving object comprehensive and reliable Information
cannot be applied to real-time processing without special hardware device	has strong adaptability on the dynamic changes in the environment	very sensitive to the irradiation which is caused by dynamic scene changes
		Advantage of not requiring previous knowledge of moving objects such as shapes or movements **Disadvantage**cannot

		discriminate moving objects from backgrounds when these backgrounds change significantly

2. THE PROPOSED METHODS

In this section, it integrates the object detector and background subtraction in to the single process of optimization which can work efficiently for moving object detection.

Moving Object detection is the basic step for further analysis of video. Every tracking method requires an object detection mechanism either in every frame or when the object first appears from stationary background object.

When working with video data, it can be helpful to select a representative frame from video and the methods can be applied to the processing of all the frames in the video. The method computes the estimated foreground and background model of frame specified by rank.

To make the problem well posed, we have the following models to describe the foreground and the background model.

Notation:

In this paper, we use following notation. $I_j \in \mathbb{R}^m$ denotes the jth frame of video sequence, which is written as a column vector consisting of m pixels.the ith pixel in the jth frame is denoted as *ij*. $D=[\ I_1,I_2,\ldots\ldots I_n] \in IR^{m*n}$ is a matrix representing all *n* frames of a sequence. $B \in \mathbb{R}^{m\times n}$ is a matrix with the same size of D ,which denotes the underlying background image. $S \in \{0,1\}^{m\times n}$ is a binary matrix denoting the foreground support :

$$S_{ij} = \begin{cases} 0, & \text{if } ij \text{ is background} \\ 1, & \text{if } ij \text{ is foreground.} \end{cases} \quad \textbf{(1)}$$

Our objective is to estimate the foreground support *S* as well as the underlying background image *B*, from the given sequence *D*. The preprocessing model is common in both modules Detection moving objects from video sequence of a fixed camera and moving camera.

Preprocessing Model:

The input to the algorithm is a sequence of video frames which convert RGB to gray-level format. The algorithm produces a binary mask for each video frame. The pixels in the binary mask that belong to the background are assigned 0 values while the other pixels are assigned to be 1.

The preprocessing module performs basic steps to process the video frames for detecting object from video. As illustrate in Figure 3

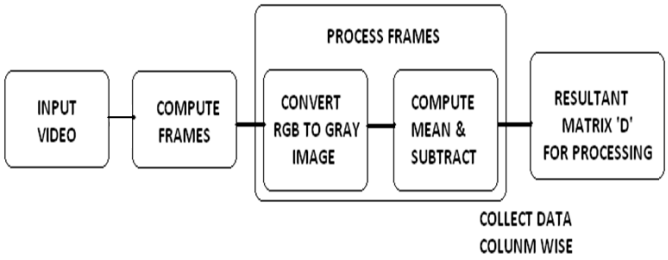


Figure 3.Framework for Preprocessing Module

The algorithm uses the Norms Matrix's which has same size as Matrix *D* of input sequences. Four norms of a matrix are used.

- ||X||o Norm: Which contains all non-zero entries
  $$||X||o= \sqrt{\sum} i|Xi|$$
- ||X||1 Norm: which computes for the difference between the two matrices and vectors.
  $$||X||o= \sum i|Xi|$$
- $||X||_F$ Norm: which compute the sum of squared difference (SUD).
  $$||X||F= \sqrt{\sum} ij|Xij|^2$$
- Nuclear Norm: which compute sum of singular value.

Transform Matrix: In Transform matrix the input matrix 'D' is processed, is used to recover the values later if the values is missing or lost after processing the video. This is the input matrix for both modules Detection moving objects from video sequence of a fixed camera and moving camera.

The transform matrix finds the variation acquire in the sequence of frames, which first compute the middle frame, then process all frames from middle to first frame and then process middle to right frame because the assumption is that the most of the variation are occurs in video at middle part.

Detecting moving objects from video sequences of a Fixed Camera:

Background refers to a static scene and foreground refers to the moving objects. Objective is to estimate the foreground support as well as underlying background images.

Steps:

- Preprocessing [Moving Object And Static Background]
- Background Model
- Estimate Low Rank matrix for Background Foreground Model
- Estimate Low Rank matrix for Foreground

The following figure 4 shows the detecting moving object in static background.

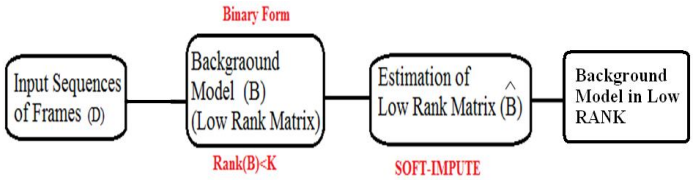


Figure 4 Detecting Moving Object In Static Background

The background intensity should be unchanged over the sequence except for variations arising from illumination change or periodical motion of dynamic textures.1 Thus, background images are linearly correlated with each other, forming a low-rank matrix B. The only Constraint on B is:

$$rank\ (B) <= K; \quad (2)$$

Where *K* is a constant to be predefined. Intrinsically, *K* constrains the complexity of the background model.

To formulate the background model, the SOFT-IMPUTE [10] method is used which produces a sequence of solutions for which the criterion decreases to the optimal solution with every iteration and the successive iterates get closer to the optimal set of solutions of the problem. SOFT-IMPUTE decreases the value of the objective function towards its minimum, and at the same time gets closer to the set of optimal solutions of the problem In many applications measured data can be represented in a matrix *Xm×n*, for which only a relatively small number of entries are observed. The problem is to "complete" the matrix based on the observed entries, and has been dubbed the matrix completion problem.

SOFT-IMPUTE iteratively replaces the missing elements with those obtained from a soft-threshold SVD. SOFT-IMPUTE algorithm , which makes use of the following lemma[] :

Lemma 1. Given a matrix Z, the solution to the optimization problem

$$\underset{Z}{\text{minimize}} \quad \frac{1}{2}\|W-Z\|_F^2+\lambda\|Z\|_* \quad (3)$$

is given by $\hat{Z}=\mathbf{S}_\lambda(W)$ *where*

$$\mathbf{S}_\lambda(W)\equiv UD_\lambda V' \quad with \quad D_\lambda=\mathrm{diag}\,[(d_1-\lambda)_+,\ldots,(d_r-\lambda)_+], \quad (4)$$

UDV' *is the SVD of* W, $D=\mathrm{diag}\,[d_1,\ldots,d_r]$, *and* $t_+=\max(t,0)$.

Using Lemma 1,the optimal solution to can be obtained by iteratively using:

$$\hat{B}\leftarrow\Theta_\alpha(\mathcal{P}_{\hat{S}^\perp}(D)+\mathcal{P}_{\hat{S}}(\hat{B})) \quad (5)$$

with arbitrarily initialized $\hat{B}$.
The foreground is defined as any object that moves differently from the background. Foreground motion gives intensity changes that cannot be fitted into the low-rank model of background. Thus, they can be detected as outliers in the low-rank representation. Generally, we have a prior that foreground objects should be contiguous pieces with relatively small size.

Algorithm: Background estimation using soft impute method.

Soft Impute :iterative soft threshold SVD to impute the missing values

Input : D=[$I_1,I_2,\ldots\ldots I_n$] € IR^{m*n}

Initialization:
'X': is incomplete matrix
'maxRank': is the desired rank in the constraint
'Omega':is the mask with value 1 for data and 0 for missing part

Steps:

```
if isEmpty(Z)
                z=x;
 end
if isEmpty(Omega)
        Omega=true(size(x))
    end
if isEmpty(maxRank)
                maxRank=-1;
end
Repeat
while(1)
        -c=x*omega+z*(1-omega)
        -apply the SVD(single value Decomposition)
        -d=diag(D)
        -index=find(d>alpha)
        -'z' recompute based on index
        -k=length(index)
Termination condition
        Repeat
        -if (k<maxRank && omega >0.0001)
                alpha=alpha+eta;
        else
                break;
        end
```

Output: smooth Background Model and masks for foreground model.

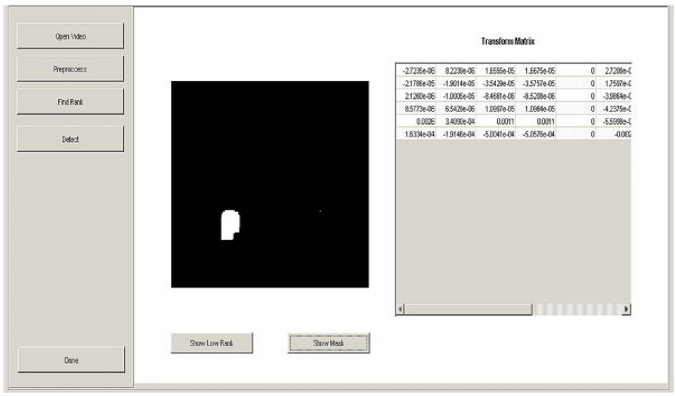


Figure 5 Mask for foreground Moving Object In Static Background

Result of soft impute method shows the mask for foreground and later this mask is used by MRF graph cut method ,for detecting the foreground in processing video.

Foreground Model Used The Markov Random Field with Graph Cut Method:

To compute the foreground model, Markov random field (MRFs) methods are used. Due to utilization of the relativity of every pixel of an image, the Markov Random Field (MRF) model is effective in solving the problem of detecting moving object under a complex background.

The Markov Random Fields (MRFs) [9] is statistical model, which used for restore the true image; images are often treated as realizations of a random process and MRFs to improve the accuracy of detecting foreground object. As illustrate in Figure 6:

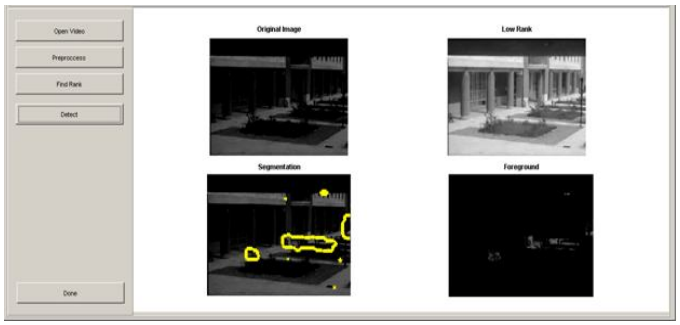


Figure 6 Segmentation of foreground Moving Object In Static Background

Detecting moving objects from video sequences of a Moving Camera:

The above section is based on the assumption that the videos are captured by static cameras and background is static and the foreground is moving. In this section, we propose the method which handles the both background and foreground are moving which is caused by moving cameras.

The proposed method uses image registration for detection moving object in motion camera. The registration is a process which makes the pixel in two images precisely coincide to the same points in the video. Once registered the image can be combined or fused in a way that improve detection of foreground in motion camera.

In this method, we use dataset having object is moving in the video with motion background and also detect the outliers present in video sequences.

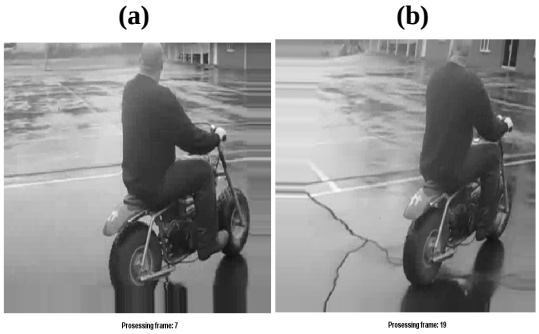


Figure 7. Moving object under motion camera (a) The processed frame 7, (b) the processed frame 19.

This case represents the most general scenario of motion because observer motion and object motion induce multiple coupled motion. As illustrate in Figure 8:

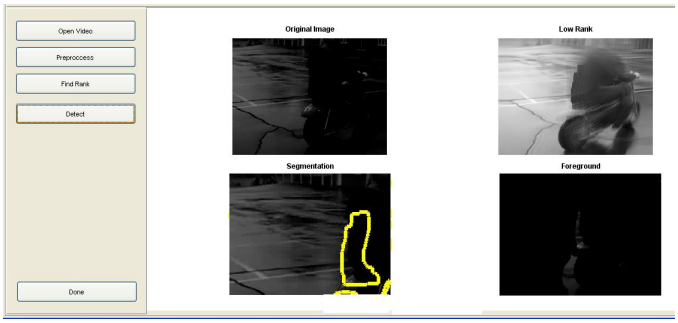


Figure 8. Segmentation of foreground Moving Object In Motion Background

3. CONCLUSION

In this paper, we discussed a variety of techniques to detect moving object in video frames. Amongst the methods reviewed, the background subtraction method; the subtraction of color and edge channels are performed separately before finding out the result. It is not robust against changes in illumination. It cannot detect non stationary background object such as swinging leaves, rain snow and shadow cast by moving object. Furthermore, in this paper, we have proposed a single process of optimization which integrates the object detection and background learning which can be used to detect

the moving object accurately, such that the time and accuracy attributes can be improved.

4. REFERENCES

[1] N. Paragios, and R. Deriche.. Geodesic active contours and level sets for the detection and tracking of moving objects. IEEE Trans. Patt. Analy. Mach. Intell. 22, 3, 266–280, 2000.

[2] A Survey on Moving Object Detection and Tracking in Video Surveillance System Kinjal A Joshi, Darshak G. Thakore International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[3] C. Stauffer and W. Grimson. Adaptive background mixture models for realtime tracking. In Proc. of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, page 246252, 1999.

[4] Sumer Jabri, Zoran Duric, Harry Wechsler, Azriel Rosenfeld, "Detection and Location of People in Video Images Using Adaptive Fusion of Color and Edge Information," In Proc. 15th Int'l Conf. on Pattern Reg, 2000,vol. 4,pp. 627 – 630.

[5] James W. Davis, Stephanie R. Taylor, "Analysis and Recognition of Walking Movements," In Proc.16th Int'l Conf. on pattern Recognition, 2002, vol.1, pp. 315 – 318.

[6] I. Haritaoglu, D. Harwood, and L. Davis, "W4: Who? When? Where? What? A real time system for detecting and tracking people". In Proc. Int. Conf. Auto. Face and Gesture Recog., 1998, pages 222– 227.

[7] A Unified Approach to Moving Object Detection in 2D and 3D Scenes Michal Irani and P. Anandan IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 20, NO. 6, JUNE 1998 577.

[8] Shireen Y. Elhabian, Khaled M. El-Sayed and Sumaya H. Ahmed," Moving Object Detection in Spatial Domain using Background Removal Techniques - State-of-Art", Recent Patents on Computer Science, 2008.

[9] Xiaowei Zhou,Can Yang, and Weichuan Yu," Moving Object Detection by Detecting Contiguous Outliers in the Low-Rank Representation", IEEE TRANSACTIONS ON PATTERN ANLYSIS AND MACHINE INTELLIGENCE, IEEE, March 2013.

[10] R. Mazumder, T. Hastie, and R. Tibshirani, "Spectral Regularization Algorithms for Learning Large Incomplete atrices," J. Machine Learning Research, vol. 11, pp. 2287-2322, 2010.

[11] A. Yilmaz, O. Javed, and M. Shah, "Object Tracking: A Survey," ACM Computing Surveys, vol. 38, no. 4, pp. 1-45, 2006.

[12]Ding Zhonglin and Lili,"Research on hybrid Moving Object Detection Algorithum in

[13] Yoginee B. Bramhe(Pethe), P.S. Kulkarni, "An Implementation of Moving Object Detection,Tracking and Counting Objects for Traffic Surveillance System," Int'l Conf. on Computational Intelligence and Comm. Networks (CICN), 2011, pp. 143 – 148.

[14] Imamura.K, Kubo.N, Hashimoto.H,"Automatic moving object extraction using x-means clustering Picture Coding Symposium (PCS),pp246 - 249 , Dec 2010.

[15] R. Li, S. Yu, and X. Yang, "Efficient spatio-temporal segmentation for extract ing moving objects in video sequences," IEEE Transactions on Consumer Electronics, vol. 54, pp. 1161-1 167, Mar 2007 .

[16] A. M. McIvor. "Background subtraction techniques", In Proc. of Image and Vision Computing, Auckland, New Zealand, 2000.

[16] D. Sappa, Fadi Dornaika, David Geronimo Antonio Lopez."Registration Based moving object detection from a moving camera ",IROS 2008 2nd Workshop: Planning , Perception and Navigation for Intelligent Vehicles.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 284 - 291, 2014, ISSN: 2319–8656

A Study of Sybil and Temporal Attacks in Vehicular Ad Hoc Networks: Types, Challenges, and Impacts

Deepika Shrivastava
DCEA, NITTTR
Bhopal, India

Ankur Pandey
DCEA, NITTTR
Bhopal, India

Abstract: In recent years, the number of automobiles on the road has increased tremendously. Due to high density and mobility of vehicles, possible threats and road accidents are increasing. Wireless communication allows sending safety and other critical information. Due to this inherent wireless characteristic and periodic exchange of safety packets, Vehicular Ad-hoc Network (VANET) is vulnerable to number of security threats like Sybil attack or temporal attack. In this paper, a detailed discussion has been done on both the type of attacks. With the help of already published works, some approaches have also been studied which have proved to be of significance in detection of these attacks.

Keywords: attacks; malicious; OBU; RSU; VANET

1 INTRODUCTION

During the past few years, there has been very rapid growth in wireless communication which has provided number of opportunity in computer networking aiming for data transfer where wired communication cannot be imagined in the real world. Wireless communication has provided the ability to communicate with the mobile devices in the continuously changing topology. This wireless communication of mobile devices has led to the creation of the term MANETs (Mobile Ad Hoc Networks).

Vehicular Ad Hoc Networks (VANET) is a special class of MANET where communicating nodes are vehicles. An ad hoc network [1] consists of group of nodes that can transmit and receive information with each other through wireless medium, either with a fixed infrastructure with or without any centralized management. Each node performs the functioning of router also. VANET differs from MANET due to its unique characteristics. Connections between vehicles are short lived. Network topology is dynamic, nodes move in and out of the range of neighboring nodes very quickly. Density of network also changes dynamically.

1.1 VANET vs. MANET

Unlike MANETs, the vehicle's mobility in VANETs is restricted by predefined roads. Vehicle's velocities are also restricted due to level of congestion on the roads, speed limitation, and traffic control mechanisms. In addition, given the fact that future vehicles can be equipped with devices with potentially longer transmission ranges, rechargeable source of energy, and extensive onboard storage capacities, processing power and storage efficiency are not an issue in VANETs whereas, this issues exits in MANETs. From these features, VANETs are considered as an extremely flexible and relatively “easy-to-manage” network pattern of MANETs.

1.2 VANET Model

A Vehicle deployed in the network contains following components. These components are displayed in Figure 1.

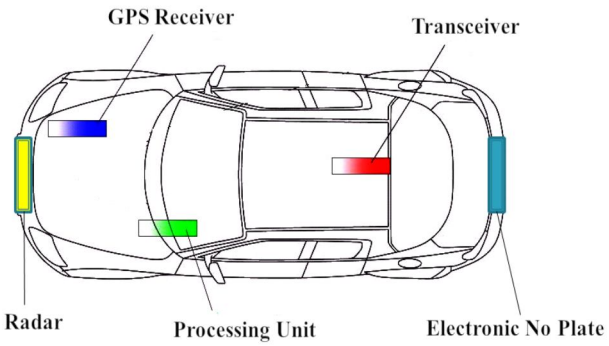


Figure 1. VANET Model

- A GPS navigation system
- Microwave radar that can detect objects at certain distance
- A computing unit, which will provide data processing, computing and storage
- A wireless transceiver, which provides standard communication for VANET
- A unique ID, such as an electronic license plate

1.3 Features of VANET

Some of the important features of the VANET are listed below:

- The movements of these nodes are very fast
- The movements of nodes are restricted by road topology
- Vehicle acts as transceiver i.e. sending and receiving at the same time while creating a highly dynamic and continuously changing network.
- The vehicular density varies from time to time. For example, density gets increased during day time and decrease at night.

2 APPLICATIONS OF VANET

The safety and security approaches of VANET have led its existence into number of applications. Figure 2 shows some of the most common applications of the VANET.

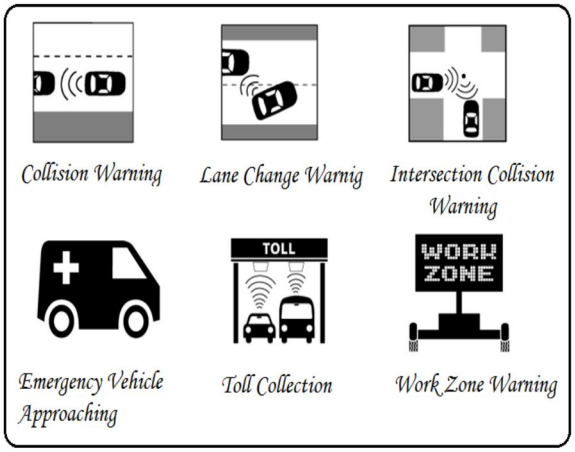


Figure 2. Applications of VANET

2.1 Increase Traveler Safety

VANET senses and provides information like intersection collision warning, lane change warning, emergency brake applied by the front vehicle warning, curve turn warning, etc, which effects the travelers safety. Traveler can take the proper measures to avoid unwanted situations like slowdown the vehicle.

2.2 Traffic Information

Warning related to traffic jams ahead, traffic signals, emergency vehicle approaching, availability of parking slot, etc, which certainly reduces the travel time and fuel consumption.

2.3 Road Condition and weather Info.

Notification of damaged road, spreading of oil, speed breaker, slippery road, weather information, landslides in the mountain regions assists the passenger to handle the unknowing situation.

2.4 Internet Access via RSUs

One can browse internet, check mail, find restaurants, gas stations, etc, in the nearby area along the road. A Roadside Services Database will be installed from the local area that will be connected to the corresponding RSUs. It thus increases the onboard luxury. Passengers may share some common interests, chat and children can play online games etc.

2.5 Electronic Toll Collection

Non-safety applications increase the overall comfort of the driver. Electronic toll collection and parking lot payment are few possible non-safety applications. Instead of driver having to stop at each and every toll booth to make a payment, the payment will be made electronically through the network. Also, a number of entertainment features have been proposed for vehicular networks, such as transferring of music and video files for in-car entertainment.

3 COMMUNICATION IN VANET

VANET communication is used to improve vehicle's passenger safety by means of inter-vehicle communication. In Vehicular Ad Hoc Network, communication is based on Dedicated Short Range Communication (DSRC) band [5]. The two types of communication devices employed in VANETs are as shown in Figure 3 –

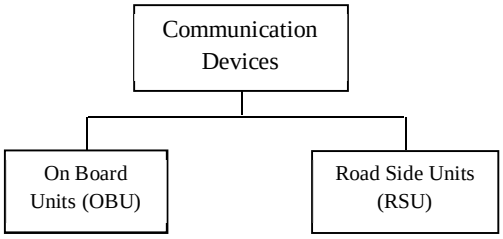


Figure 3. Communication Devices Deployed in VANET

- Vehicles or On Board Units (OBUs)
- Road Side Units (RSUs) are fixed infrastructure on the road

3.1 VANET Architecture

An instance of the architecture of vehicular network is as shown in Figure 4.

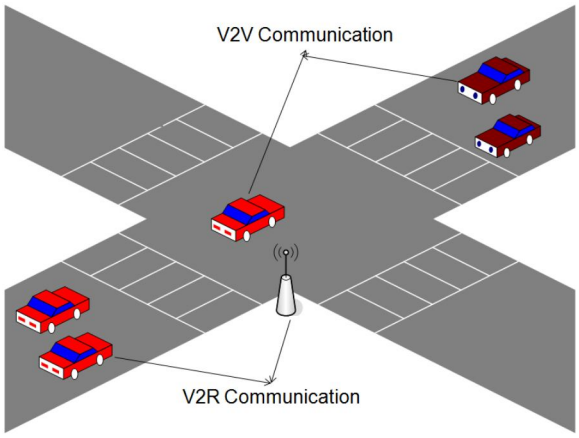


Figure 4. VANET Architecture

- Vehicle to Vehicle (V2V): Vehicles communicates with each other through wireless medium.
- Vehicle to Road side unit (V2R): Vehicles communicates with fixed infrastructure via wireless communication.
- Road side unit to Road side unit (R2R): A RSU communicates with another RSU through wired channel.

3.2 Safety Message Transmission

VANET is needed for automated and intelligent Transportation Systems (ITS). In the case of an accident, inter vehicle communication can be used to warn other vehicles approaching

the site. Each node in VANET periodically broadcasts beacon packets to announce its presence to neighboring nodes. Each beacon packet contains sender identity, position, time-stamp and speed etc. A safety message is shown in Figure 5. The difference between the beacon packets and safety packets is that the former does not have warning field and safety packets are sent only on the occurrence of specific event.

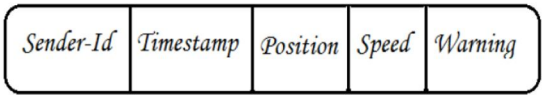


Figure 5. A Safety Message Format

Two kinds of message transmission take place in VANET –

- Periodic messages or Beacon Packets: They are sent with the intention of providing non-critical information (e.g. Sender-ID, GPS position, speed, direction etc). These packets are broadcasted at a regular time interval.
- Event-driven messages or Safety Packets: Event-driven messages are those messages which are generated on the occurrence of certain life critical incident (e.g. lane change or braking of the front vehicle)

3.3 Wireless Radio Channel

The wireless radio channel makes a great impact on the reception of packets. Path loss and shadowing causes the fluctuation in the received signal strength. Path loss [6] is caused by dissipation of the power radiated by the transmitter as well as due to the effects of the propagation channel. Shadowing is due to obstacles between receiver and transmitter that attenuate signal power through reflection, absorption, scattering and refraction. Both path loss and shadowing are caused due to long distances therefore they are considered as large-scale propagation effects.

Multipath is due to the receiving of multiple components of the signal. These components may be attenuated, delayed, shifted in phase and/or frequency from the LOS (Line of Sight) signal path at the receiver. Variations due to multipath are considered as small-scale propagation effects as they are on the order of the wave length. There exists number of different models for signal propagation between the receiver and the transmitter. Some models are mentioned below:

- Free Space Model
- Ground Reflection Model
- Shadowing Model
- Empirical Path Model

4 Wireless Technology in VANET

Here the wireless technologies have been divided into two broad categories. On one side, there are large area technologies as GSM, GPRS or UMTS, which have moderate bandwidth. On the other side, there is much higher bandwidth than the local area technologies such as WLAN (Wireless Local Area Network). There exist two different standards for Wireless LAN i.e. HIPERLAN from European Telecommunications Standards Institute (ETSI) and 802.11 from Institute of Electrical and Electronics Engineers (IEEE).

Nowadays, the 802.11 standard totally dominates the market and the implementing hardware is well engineered. Local Area Networks (LAN) and Metropolitan Area Networks (MAN) are standardized under the IEEE 802.11 WLAN protocols, which is the part of the IEEE 802 family. The IEEE 802 family has Internet Protocol (IP) layer with its routing protocols, e.g. AODV or DSR for mobile ad hoc networks, Logical Link Control layer (LLC), MAC (Medium Access Control) layer and finally PHY (Physical) layer. Figure 6 shows the OSI layered model of VANET.

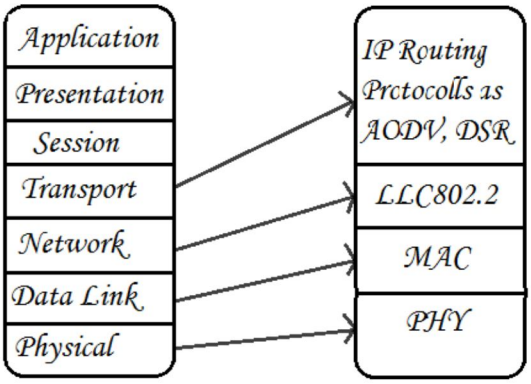


Figure 6. OSI Model for Wireless Communications

The IEEE 802.11 standard is constructed for wireless local area network technology (WLAN). Currently, 802.11 describe two specific operational modes. These modes are infrastructural and infrastructure-less based networks. The infrastructure-less based networks has been generally termed as Ad-hoc networks. Ad-hoc networks use Wi-Fi technology for Internet connectivity. It relies on the information distributed through a cluster of interconnected vehicles to transport, share, and receive information. The IEEE 802.11p standard is the adaption of the 802.11 protocol for WAVE (Wireless Access in Vehicular Environments).

5 Security Constraints in VANET

There are number of challenges in implementing security techniques in VANET. Few of the significant ones are listed below:

5.1 Equilibrium between Authentication and Privacy

For authentication of all message transmission, the identification of the vehicle from which message has been sent is required to track down. In general, people will not like to reveal their privacy to others; therefore this has to come in equilibrium. Therefore a system needs to be introduced which keeps the balance between the authentication of message and privacy of an individual.

5.2 High Mobility

Due to high mobility and rapidly changing topology, the protocol cannot be based on handshaking. So, it's a real challenge to implement and maintain the network.

5.3 Real-time Guarantees

As the major VANET applications are used for collision avoidance, hazard warning and accident warning information, so applications require strict deadlines for message delivery.

5.4 Central Authority

All the VANET nodes i.e. the vehicles are required to register with a central authority and already have a unique identity in the form of a license plate. Central Authority is a kind of infrastructure which maintains records of all vehicles.

6 SAFETY REQUIREMENTS FOR VANET

There are many safety requirements which should be taken in order to ensure safety of the passengers and the vehicle. Few significant safety requirements are discussed below:

6.1 Authentication

Authentication is required in VANET to assure that the messages are sent by the actual nodes. So, the effect of attack by greedy drivers and other adversaries can be reduced to a greater extent. Basic authentication scheme include attaching the sender's identity, it raises privacy concerns, as it would allow tracking of vehicles.

6.2 Message Integrity

This is required to ensure that the packet/data has not been tampered or altered after it was generated. Integrity is not only concerned with the original source of data but also whether it has been modified since its creation.

6.3 Message Non-repudiation

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends [2].

6.4 Entity Authentication

It is required to ensures that the message received is not very old i.e. the message is send within a very short period. It ensures that the sender who has generated the message is still inside the network.

6.5 Access Control

It specifies the roles and privileges to be given to the nodes in the network and what each node can do in the network and what messages can be generated by it.

6.6 Message Confidentiality

It is a system which is required when certain information need to be kept private. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist.

6.7 Privacy

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information.

6.8 Real-time Guarantees

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met.

7 ATTACKS ON VANET

Incorrect information sent by a malfunctioning or attacker node might jeopardize the security and safety of the vehicles and endangers other vehicle's approaching the site. Emergency vehicle warning would have to be compromised without assurance that transmission is done from an actual emergency vehicle. Thus, it is challenging job to identify if the node spreading traffic safety information is malicious or not.

7.1 Bogus Information

Attacker sends inaccurate information into the network in order to achieve personal benefit. Selfish vehicles may attempt to clear up the path ahead with false traffic reports to reach his destination in the shortest possible time; criminals being chased by the police may disseminate the bogus information to other vehicles in order to block police cars, and terrorists may produce serious traffic collisions with contradictory traffic announcements.

7.2 Imposture

Attackers pretend or use other vehicle's identity to create illusion. For example, a vehicle may pretend to be a fire brigade or police car or ambulance van to free the traffic flow for its benefits. This type of attack is usually performed to impersonate a legitimate vehicle or RSU.

7.3 Denial-of-Service

Attacker may deny the other vehicles to use the VANET network by channel jamming or aggressive injection of dummy message.

8 TEMPORAL ATTACKS

Temporal attacks stands for time related attacks like, delay in packet forwarding and repeating the packet sent at earlier time interval. There are three types of temporal attacks. Each type of temporal attack is explained below:

8.1 Replay Attack

An attacker can replay the received packets apart from acting as a normal node (forwards all the received packets). In this attack, packets are fraudulently repeated. This operation is carried out by a malicious node that intercepts the safety packet and retransmits it. This type of attack is usually performed to impersonate a legitimate vehicle or RSU. Since, Basic 802.11 security does not contain sequence numbers; therefore it provides no protection against replay. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system.

A typical replay attack scenario in VANET is shown in Figure 7. Attacker is repeatedly sending the message send by vehicle V1 to vehicle V2.

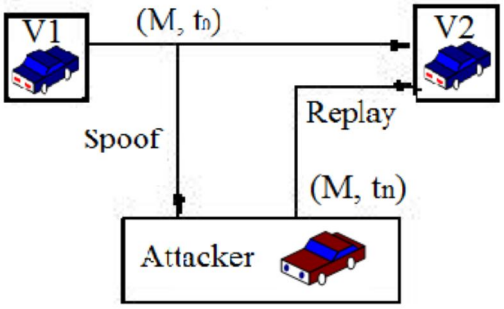


Figure 7. Packet Replay Attack

8.2 Delay Attack

In this attack, a vehicle delays the packet being forwarded by certain time duration in the network. It is more harmful than replay attack as vehicles may not get enough time to respond to particular emergency situation. For Example: Attacker node N_a observes 'CLEAR ROAD' ahead at time t_0. Instead of forwarding the 'ROAD IS CLEAR' message to the other vehicles in the road; it introduces the delay of time t_d. Suppose after t_d time there is congestion in the road, but the attacker node Na will forward the packet observed at time t_0. The other vehicle instead of decreasing the speed they will increase their speed after receiving the delay message 'TRAFFIC JAM'. This will lead to severe results like loss of life and property. Figure 8 shows the delay attack on VANET.

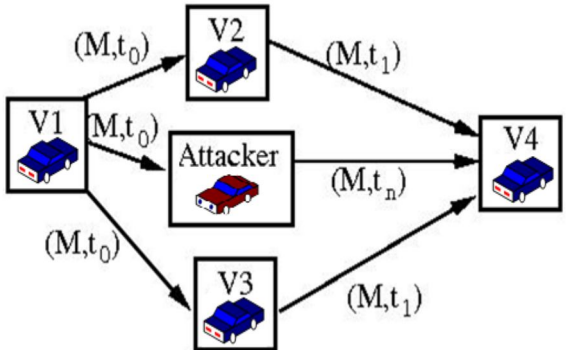


Figure 8. Packet Delay Attack

8.3 Suppression Attack

In this attack, an attacker selectively drops packets received from the neighbors, these packets may hold critical safety related information for the receiver, the attacker suppress or block these packets and can use them again at later time [10]. Such type of attack can prevent warning messing to be forwarded. For instance, an attacker may block a congestion warning, so vehicles will not receive the warning and forced to wait in the traffic for the long time. Figure 9 shows the suppression attack on VANET.

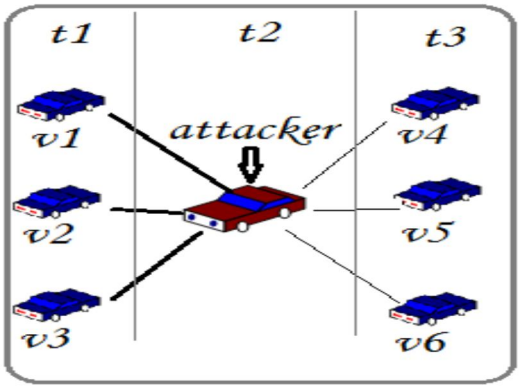


Figure 9. Packet Suppression Attack

8.4 Related Work

This section explores the previous work done on temporal attacks and their detection approaches in VANET. It is a normal phenomenon to forward each received packet to neighboring nodes VANET. Malicious nodes can adversely impact this process by purposely interfering in-between the packet transfer among the vehicles.

In [3] Aijaz et. al. have presented various types of attacks on inter-vehicle communication systems. They analyzed how an attacker can modify the sensor readings and the input of an on-board unit (OBU). Here, the authors proposed plausibility checks using constant system examinations, but no detailed discussion on implementation of plausibility check is presented. In [13] M. Raya and J.P. Hubaux have discussed number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and security problems.

In [4] Nai-Wei et. al. have presented an illusion attack in VANET. In this attack, a malicious node creates a particular traffic situation and sends fraud traffic warning messages to other nodes for convincing them that a traffic event has occurred. To detect and defend against the illusion network, plausibility validation network model is introduced in this paper. However, they did not implement this attack and its defense approach in any simulator. In [27] Yan et. al. have proposed a position verification approach for detection of position related misbehaviors.

In [28][29] Raya et. al. have suggested the use of VPKI (Vehicular Public Key Infrastructure) as a solution, where each node will have a public/private key. When a vehicle sends a safety message, it signs it with its own private key and adds the Certificate Authority (CAs) certificate. In [30] Ren et. al. have proposed the use of the group signature, but the biggest disadvantage of this method is its overhead because every time any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted. Another issue is that VANET mobility prevents the network from making a static group, as topology is dynamic in nature.

In [14] Golle et. al. have proposed an approach to detect and correct malicious data in VANET. They assume that vehicular

node is maintaining a model which consists of all the information that nodes has about the network. When a node receives a message, it compares received message with VANET model. If the received message does not comply with the VANET model, it is considered an invalid message. This approach requires gathering of sufficient messages to perform fraud message detection and suspicious data correction. The VANET model used in this paper is predefined and not flexible to switch to a new one. It is not feasible to design a model based on global knowledge of the network. Schmidt et. al. [33] constructs reputation models for other vehicles based on the claims from sending vehicles. In this way, they create a model of normal behavior of nodes in VANET. If the behavior of a node differs from the normal behavior, it is marked as suspicious.

9 SYBIL ATTACK

A Sybil attack is a type of attack in which a malicious node illegitimately fabricates multiple vehicle identities. In a Sybil attack, there are two types of nodes that are malicious node or Sybil attacker and Sybil node as shown in Figure 10.

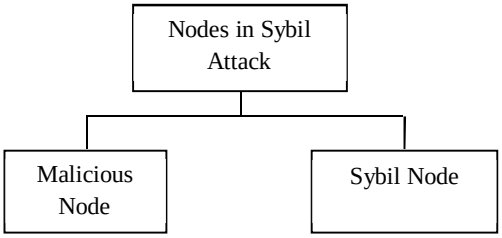


Figure 10. Nodes Participates in Sybil Attack

- Malicious node/Sybil attacker: The node which spoofs the identities of other nodes.
- Sybil node: Additional identities created by the malicious node are known as Sybil nodes.

Figure 11 shows the typical Sybil attack in VANET scenario. Sybil attacker is spoofing the identities of A, B, and C. The impact of Sybil attack gets severe when all identities created by attacker participate simultaneously in the network. Sybil attack is classified into two categories. Both of them are explained below:

Case 1: When Sybil attacker creates the identities of actually existing node in the network. Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case $S \subseteq N$.

Case 2: When Sybil attacker creates the identities from outside the network. Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case $S \not\subset N$.

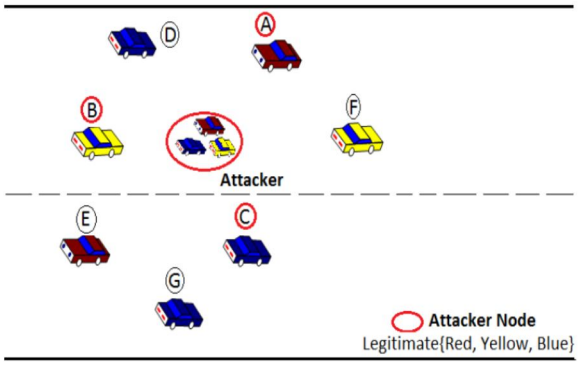


Figure 11. Sybil Attack in VANET

As messages are broadcast over the shared communication media, it is easy for a malicious node to get additional identities either by stealing or fabricating them. The main motive of Sybil attack detection approach is to ensure that each physical node is bound with only one valid identity.

9.1 Related Work

VANETs are vulnerable to many security threats and attacks. Various types of attacks in VANET are presented in [3][4]. An opponent or attacker may secretly listen on the channel easily and modify or insert the wrong information in the network. It is a normal phenomenon to forward each received packet to neighboring nodes VANET. Malicious nodes can adversely impact this process by purposely interfering in-between the packet transfer among the vehicles. Sybil attack is one of the major concerns in the VANET scenario. In Sybil attack, a malicious node illegitimately spoofs the identities of other nodes. It pretends or impersonates the original node to benefit itself.

In [11], Douceur et. al. was the first to describe and formalize the Sybil attack in the context of peer to peer networks. It can easily defeat reputation and threshold protocols intended to protect against it. In [12] resource testing was one of the methods proposed to defend a Sybil attack. It is assumed that physical resources of each node are limited. Unfortunately, this method is not suitable for Ad Hoc networks because an attacker can have more resources than honest nodes. Some papers such as [13][14] introduced the use of Public Key Infrastructure (PKI) algorithms for VANETs in which public key cryptography is used to provide solution to the security problem in VANETs.

In [15] a multi-factor authentication scheme is used in addition to public key information. A certificate is issued to all vehicles. These contain not only the public key information but also contain a set of physical attribute values of a vehicle, such as transmitter coverage, radio frequency fingerprint and so on, recorded by CA. In [16] Hubaux et. al. have introduced verifiable multilateration method for performing distance bounding. In this approach, two or three fixed units (RSUs) are used to perform distance bounding. This method is not a very appropriate method to detect Sybil attack as it involves RSUs as a key player in detection mechanism. This method is more infrastructures dependent.

In [17] Demirbas et. al. have presented a Sybil attack detection scheme in wireless sensor networks using multiple sensors Received Signal Strength Indicator (RSSI) measurements. However, it does not mention how to identify honest neighboring nodes. This scheme cannot be applied in situations where nodes are moving, not trusted or may collude in hostile environment. The method suggested in [18][19] requires some trusted monitors for observing the behavior of nodes in a network. This is not realistic in VANET because the Sybil attacker may penetrate these trusted observing nodes and these Sybil nodes will report fake data. A secure hardware based method is proposed in [20] which are built on trusted platform module (TPM). Secure information is stored in shielded locations of the module, where any type of forging or modification of data is impossible. Hence, communication between TPMs of the vehicles is protected from the Sybil attack.

In [21] Guette et. al. have analyzed the effectiveness of Sybil attack in various assumptions of transmission signal tuning and antenna. They showed the limitation of RSS based Sybil attack detection in VANET. In [22] Xiao et. al. have proposed a localized and distributed scheme to detect Sybil attacks in VANETs. The approach takes advantage of VANET traffic patterns and road side base stations. In [23] Zhou et. al. have proposed a privacy preserving method for detecting a Sybil attack with trustable roadside boxes and pseudonyms. Vehicles are assigned a pool of pseudonyms from a centralized unit, which are used for generating traffic messages instead of real identities for privacy reason. Pseudonym belonging to a vehicle is hashed to a unique value. Vehicles cannot abuse these pseudonyms for a Sybil attack. This scheme provides privacy but it is based on the assumption that individual vehicles are registered and managed by trusted authorities.

In the approach discussed in [24][25], RSUs are the only components that issue the certificates to all vehicles passing across them. It is very rare to have two vehicles passing by multiple RSUs at exactly the same time due to the difference of moving dynamics of multiple vehicles. Two messages will be treated as a Sybil attack issued by one vehicle if they have similar time-stamp series issued by RSUs. In [26] Shaohe et. al. have proposed a cooperative RSS based Sybil attack detection for static sensor networks where all nodes have fixed transmission power either it are honest or malicious. This approach does not rely on the accurate position of the nodes rather relative distance among the nodes is used. Each node overhears packets and computes the distance to other nodes using received signal strength. In [7] Jyoti et. al. have proposed and implemented RSS-based Sybil attack detection technique in VANETs. The detection method was based on the similarity in RSS value received by the RSUs.

10 CONCLUSION

Malicious nodes are harmful for proper functioning of VANET applications. If correct traffic information is not delivered to the drivers before the vehicle approaches to the location of occurred event, critical problems can significantly alleviate. In Sybil attack, a malicious node forges multiple or fake identities (either present in the network or not), in order to disrupt the proper functioning of VANET applications. It creates an illusion on road, leading to disruption in the network scenario. In Temporal attacks, a malicious node either impedes or delays the forwarding of critical safety messages received from neighboring nodes. It can also perform replay attack by repeatedly sending the information of events occurred earlier. In this paper, both the attacks are discussed in detail and their solutions which have been proposed in previous studies are mentioned.

11 REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference. In Ad Hoc Wireless Networks: Architectures and Protocols, 2007.

[2] Antonios Stampoulis, Zheng Chai, “A Survey of Security in Vehicular Networks”.

[3] Amer Aijaz, Bernd Bochow, Florian Dtzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmller, “Attacks on Inter Vehicle Communication Systems - an Analysis”, In Proc. of WIT, pp. 189-194, 2006.

[4] Nai-Wei Lo, Hsiao-Chien Tsai, “Illusion Attack on VANET Applications - A Message Plausibility Problem”, In Proc. of IEEE Globecom Workshops, pp. 1-8, 2007.

[5] Jiang, L. Delgrossi, “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments”, In Proc. of Vehicular Technology Conference (VTC), pp. 2036-2040, 2008.

[6] A. Goldsmith, Wireless communications. In Cambridge University Press, 2005.

[7] Jyoti Grover, Nitesh Prajapati, Manoj Singh Gaur, and Vijay Laxmi, “RSS-based Sybil Attack Detection in VANETs”, In IEEE Proc. of the International Conference (TENCON), pp. 2278-2283, 2010.

[8] Nitesh Kr. Prajapati, Jyoti Grover, and M.S Gaur, “Implementation of Temporal Attacks in Vehicular Ad Hoc Networks”, International Conference on Electronic, Information and Communication Systems Engineering (ICEICE2020) 28-30 March, Jodhpur, India.

[9] Jyoti Grover, V.Laxmi, M.S Gaur and Nitesh Kr. Prajapati, “A Distributed Sybil Attack Detection Approach using Neighboring Vehicles in VANET”, The Computer Journal (Oxford), Special Issue on Security and Privacy in Innovative Communication and Services.

[10] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks”, In Proc. of HotNets-IV, 2005.

[11] John R. Douceur, “The Sybil Attack”, In IPTPS 01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, London, UK, 2002. Springer-Verlag.

[12] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses”, In IPSN '04: Proceedings of the 3rd International Symposium on Information processing in Sensor Networks, New York, USA. ACM.

[13] M. Raya and J.P. Hubaux, "Securing Vehicular Ad-hoc Networks", Transactions of Journal of Computer Security, Vol. 15, Issue 1, pp. 39-68, 2007.

[14] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and Correcting Malicious Data in VANETs", In Proc. of 1st ACM International workshop on Vehicular Ad-hoc Networks, pp. 29-37, New York, USA, 2004, ACM.

[15] S. Pal, A.K. Mukhopadhyay, and P.P. Bhattacharya, "Defending Mechanisms against Sybil Attack in Next Generation Mobile Ad Hoc Networks", Vol. 25, pp. 209-214. IEEE Technical Review, 2008.

[16] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, "The Security and Privacy of Smart Vehicles", In IEEE Proc. of Security and Privacy, pp. 49-55, 2004.

[17] Murat Demirbas and Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", In Proc. of International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM), pp. 564-570, 2006.

[18] Chris Piro, Clay Shields, and Brian Neil Levine, "Detecting Sybil Attack in Mobile Ad hoc Networks", In Proc. of Securecomm and Workshops, pp. 1-11, Sept. 2006.

[19] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham D. Flaxman, "SybilGuard: Defending against Sybil Attacks via Social Networks", Transactions of IEEE/ACM Transition Networks, Vol. 16, Issue 3, pp. 576-589, 2008.

[20] Gilles Guette and Ciaran Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", pp. 106-116, 2008.

[21] Gilles Guette and Bertrand Ducourthial, "On the Sybil Attack Detection in VANET", In IEEE Proc. of International Conference on Mobile Ad-hoc Networks and Sensor Systems, pp. 1-6, 2007.

[22] Bo Yu Bin Xiao and Chuanshan Gao, "Detection and Localization of Sybil Nodes in VANETs", In Proc. of the Workshop on Dependability Issues in Wireless Ad-hoc Networks and Sensor Networks, pp. 1-8, New York, USA, 2006, ACM.

[23] Tong Zhou, R.R. Choudhury, Peng Ning, and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks", In Proc. of Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), pp. 1-8, Aug. 2007.

[24] B.Turgut, D.Zou, C.C. Soyoung, and Park Aslam, "Defense against Sybil Attack in Vehicular Ad-hoc Network based on Roadside Unit Support", In IEEE Proc. of Military Communications Conference (MILCOM), pp. 1-7, 2009.

[25] Chen Chen, Xin Wang, Weili Han, and Binyu Zang, "A Robust Detection of the Sybil Attack in Urban VANETs", In IEEE Proc. of ICDCS Workshops, pp. 270-276, 2009.

[26] Xin Zhao, Shaohe Lv, Xiaodong Wang, and Xingming Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", In IEEE Proc. of International Conference on Computational Intelligence and Security (CIS), 2008.

[27] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, "Providing VANET Security through Active Position Detection", Transactions of Computer Communications, Vol. 31, Issue 12, 2008.

[28] M Raya, P Papadimitratos, and J.P. Hubaux, "Securing Vehicular Communications", In IEEE Transactions of Wireless Communications, Vol. 13, Oct. 2006.

[29] M. Raya and J. P. Hubaux, "The security of VANETs", In Proc. of 2nd ACM International Workshop on Vehicular Ad-hoc Networks, 2005.

[30] W Ren, K Ren, W Lou, and Y Zhang, "Efficient User Revocation for Privacy-aware PKI", In Proc. of 5th International Conference (ICST), 2005.

[31] R. K Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer, "Vehicle Behavior Analysis to Enhance Security in VANETs", In Proc. of Vehicle to Vehicle Communication (V2VCOM), 2008.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 292 - 295, 2014, ISSN: 2319–8656

Functional Coverage for Low Power DDR2 Memory Controller in UVM

Nishanthi G
Dept. of Electronics and Communication
BNM Institute of Technology
Bangalore, India

Yasha Jyothi M Shirur
Dept. of Electronics and Communication
BNM Institute of Technology
Bangalore, India

Ramudu B
Graphene Semiconductors India Pvt Ltd
Bangalore, India

Abstract: It is a well-known fact today that verification consumes approximately 70% of the product cycle and it is one of the main hindrance in developing a complex design. The advanced CAD tools reduces the design time but still the verification time is increasing with the design complexity. Writing directed tests for every feature of a complex design is a mind-numbing task. To alleviate this, constrained random verification is done. To check if all the design specifications are covered by these several random test cases a metric called Functional Coverage is needed. This metric gauges the progress of the verification and indicates if the destination is reached. This paper presents the development of functional coverage model for Low Power Double Data Rate 2 Memory Controller [LPDDR2 MC] in Universal Verification Methodology [UVM]. In this design there are 33 AXI v1.0 compliant masters which can write/read to/from a single memory. The LPDDR2 MC and the LPDDR2 memory model is JESD209-2F [JEDEC-standard] compliant. Hence the challenge is in identifying all the functional coverage points as per the specifications of this Design under Verification [DUV]. In this paper coverage models for AXI master interface and memory interface are implemented. 100% functional coverage was achieved when all the test cases were fired. Even after adding extra test cases functional coverage remained constant. The coverage models are reusable and thereby reduces verification time.

Keywords: Functional coverage; AXI; UVM; LPDDR2 MC; DDR2 memory model; DUV

1. INTRODUCTION

Functional verification plays a key role in a product cycle. It checks if the design intent is retained in it its implementation. For complex designs there will be huge number of specifications. So writing individual test cases for all the design features is a complicated task. Only way to ease this is through constrained random stimulus generation so that thousands of tests can be generated automatically in the simulation environment. To know which functionality is exercised by these random test cases numerous waveforms should be analyzed after each simulation. This is again a wearisome task. Hence, functional coverage is needed to determine what functionality was implemented in the test case without the need of visual examination of the waveforms.

Figure 1 shows the flow of functional coverage based verification.

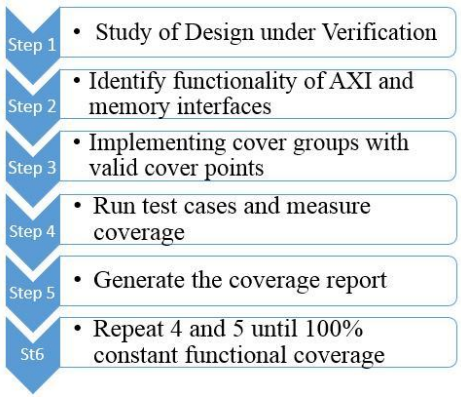


Figure 1. Flow of functional coverage of LPDDR2 MC

The cover group mechanism is coded in System Verilog and the verification methodology followed is UVM which is standardized by Accelera.

The UVM environment consists of different verification components. A verification component is a ready-to-use, configurable verification environment for a full system, design sub module or an interface protocol [3]. It can be customized as per the design behavior which makes it reusable. Coverage model is one of such verification component.

The paper is organized as follows. Section 2 describes the DUV. Section 3 describes the coverage model in UVM and the identified cover points.

2. DESIGN UNDER VERIFICATION

Figure 2 shows the simplified block diagram of LPDDR2 memory controller, it is used to drive LPDDR2 SDRAM. LPDDR2 devices use a double data rate architecture on the command/address bus to reduce the number of input pins in the system [2]. This supports 33 AXI compliant. The chosen memory model follows JEDEC standard. Hence, the memory controller can support LPDDR2 memory devices operating in a frequency range of 100MHz to 533MHz and of capacity 64 Megabits 8 Gigabits comprising 8 memory banks [2].

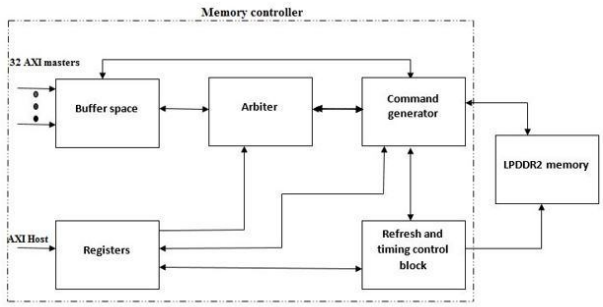


Figure.2 Simplified block diagram of LPDDR2 MC

The design flow is as follows. First the AXI host master will configure the register block. After the host configuration is complete, initialization of the memory takes place through refresh and timing control block.

Second the masters writing/reading to/from the memory will take place.

2.1 Functional coverage at interfaces

Figure 3 shows the interfaces with reference to the top module of the DUV with AXI interface and memory interface signals where the functional coverage is measured. The functionalities of the AXI protocol and the memory interface signals were identified to create a coverage model.

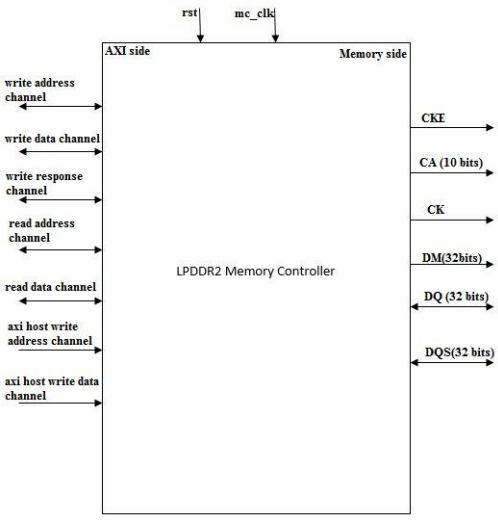


Figure.3 Interfaces of LPDDR2 MC

On the AXI side, one master has 5 channels through which the data transactions occur. The write/read address channels will carry address and control information to/from slave. The read data channel will carry both data and read response from the slave to the master. The write response channel will carry the write response for write transactions from slave to master [1]. The slave here is the memory controller.

On the memory side the CKE is the clock enable pin which will trigger the memory's clock. CA is the command/address bus which consists of bank, row, and column address information. CK is the clock signal to the memory which will be triggered from the memory controller block. DM (32 bits) is the data mask signal which indicates the valid data to and from the memory. DQS (32 bits) is the data strobe signal which indicates on which line the data is available to and from the memory.

3. COVERAGE MODEL IN UVM

3.1 UVM environment

Figure 4 shows the UVM environment diagram where the coverage collector is one of the verification component. This coverage model which is implemented in this paper gets inputs from both the AXI and memory monitor.

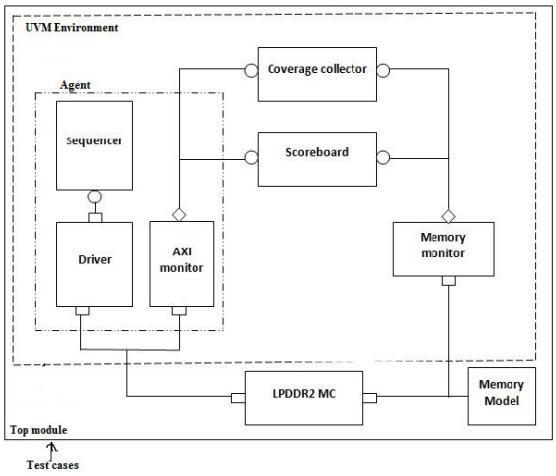


Figure.4 coverage collector in UVM environment

The environment consists of AXI agents, score board, coverage collector. The AXI universal verification component [UVC] also called as agent consists of sequencer, driver and monitor. Driver will drive the DUV with the transactions. The sequencer will control the transactions provided to the driver. Both memory and AXI monitors will monitor and collect the transactions whenever observed on the DUV interfaces. There are 33 AXI agents with monitors in each and one memory monitor and one Score board for data integrity check.

3.2 Coverage collector

Monitors will observe the transactions on all the interfaces and it will write into the coverage collector. The communication which happens in the UVM environment is transaction level modelling [TLM]. Coverage collector consists of different cover groups like AXI master cover group, AXI host cover group and Memory cover group. These cover groups has identified cover points on both the interfaces with respect to the design specifications. Each cover point will have coverage bins like valid, illegal and ignore bins. These bins are the check points which will be updated as per the received transactions. When enabled, each test case will generate a coverage database. After running all the test cases, different test cases databases are merged into a single data base. From this the overall coverage report is generated.

3.2.1 Communication between monitor and coverage collector

The TLM port connection between monitor and coverage collector is indicated by a diamond symbol at the monitor and a circle at the coverage collector. The diamond symbol is the analysis port and the circle is the port. One analysis port can be connected to any number of ports. The analysis ports will call a write function at the end of every transactions. This

write function is implemented in the coverage collector. The write function will sample the cover groups

3.2.2 AXI master cover group

In this cover group the cover points related to the AXI channel signals are identified for one master and instantiated for 32 times. For one master identified cover points are 20. The table 1 shown below shows the cover points of write address channel for this cover group.

Consider the cover point Burst type. It is a 2 bit signal which indicates the type of burst transaction. 00 for fixed, 01 for incremental, 10 for wrapping and 11 is reserved. According to the design specification the burst type followed is incremental. Therefore the valid bin is 01, invalid bin is 00 and 10, ignore bin is 11. If this cover point was not identified and if the test case did not exist for this functionality the design response will not be known. It means that there can be a bug in the design which was not verified even though the other test cases passed.

Table 1. AXI read/write cover group

Cover points in AXI read/write cover group	Description
Write address id	This checks if the number of transaction if from 1 to 16 is covered
Burst length	This checks if the data transfers within a burst covers all the length from 0 to 15
Burst size	This checks the number of data bytes within a beat covers all the size from 1 to 128 bytes
Burst type	This checks if the burst type wrapping, fixed and incremental is covered

3.2.2.1 AXI host interface cover group

In this cover group the cover points related to the AXI Host master signals are identified. The host master configures all the registers in the design to a default value. This will be the 33rd master. Identified cover points are 37. The table 2 shown below shows some of the cover points.

Table 2. AXI host cover group

Cover points in AXI host cover group	Description
Power down	This checks if the power down condition is covered
Read and write latency	This checks if all the read and write latency values are covered
Device density	This checks if all the device density from 64Mb to 8Gb is covered
Memory burst length	This checks if all the burst length 4,8,16 is covered

3.2.3 Memory interface cover group

In this cover group the cover points related to the memory interface are identified. Here the identified cover points are huge in number as there are 8 banks in the memory and there are different commands. This cover group checks for different memory commands like activate, pre-charge, write, read etc. are covered or not. This also covers the transition coverage like if a write or read operation occurred in the same memory bank back to back. This cover point is important because there might be a case where the write occurred say to bank 1 but a read did not occur to the same bank which will again indicate a presence of bug. Hence all the identified cover points are critical. Identified cover points are 248. Few of them are shown in the table 3 below.

Table 2. Memory cover group

Cover points in memory cover group	Description
Write after write in bank 0	This checks the transition coverage if there is back to back write in bank 0
Pre-charge all banks	This checks if all the banks are pre-charged (closed) condition occurred
Activate bank 1	This checks if the condition to activate bank 1 is occurred
Refresh all banks	This checks for the condition if all banks are refreshed

4. RESULTS AND ANALYSIS

For every test case coverage report was generated, 1st the illegal bins were analyzed to check if any test cases are out of the design specifications. Once the illegal bins are cleared all the valid bins are checked. Valid bins indicate the valid and critical functionality. If any valid bin was not hit, the test case was run with random seeds or run with missing test cases. The coverage report was merged once all the test cases were fired.

Figure 5 shows the screen shot of the functional coverage of the AXI write address channel. The cover point burst type is not covered as the valid bin is not hit indicating a missing test case. The overall AXI coverage is 54.54% because some of the other cover points were not covered.

Covergroup instance:\/test/#ublk#0#181/cg			100.00%	54.54%	54.54%
Coverpoints / Bins	At Least	Hits	Goal	Coverage	% of Goal
Coverpoint: write_burst_length (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
bin valid	1	3		Covered	--
Coverpoint: write_burst_size (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
illegal_bin illegal	1	1		Occurred	--
bin valid	1	2		Covered	--
Coverpoint: write_burst_type (covered 0 of 1 bins) (missing 1 of 1 bins)			100.00%	0.00%	0.00%
illegal_bin illegal	1	1		Occurred	--
ignore_bin ignore	1	2		Occurred	--
bin valid	1	0		ZERO	--
Coverpoint: write_addr_id (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
bin valid	1	3		Covered	--

Figure 5 Burst type uncovered

After running the missing test case the burst type valid bin was hit and also the other cover points were covered. Figure 6 shows the screen shot of the same.

Covergroup instance:\/test/#ublk#0#181/cg			100.00%	100.00%	100.00%
Coverpoints / Bins	**At Least**	**Hits**	**Goal**	**Coverage**	**% of Goal**
Coverpoint: write_burst_length (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
bin valid	1	30		Covered	--
Coverpoint: write_burst_size (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
illegal_bin illegal	1	11		Occurred	--
bin valid	1	19		Covered	--
Coverpoint: write_burst_type (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
illegal_bin illegal	1	21		Occurred	--
ignore_bin ignore	1	4		Occurred	--
bin valid	1	5		Covered	--
Coverpoint: write_addr_id (covered 1 of 1 bins) (missing 0 of 1 bins)			100.00%	100.00%	100.00%
bin valid	1	30		Covered	--

Figure 6 Burst type covered

5. ACKNOWLEDGMENTS

Our thanks to the BNMIT and Graphene management who have contributed towards this paper.

REFERENCES

[1] AMBA AXI protocol V1.0.

[2] JESD209-2F specifications.

[3] UVM user guide 1.1.

[4] System Verilog LRM IEEE 1800-2005.

[5] Yang Guo, Wanxia Qu, Tun Li, Sikun Li ,National University of Defense Technology, P. R. China, IEEE International conference, 2007. Coverage Driven Test Generation Framework for RTL Functional Verification.

[6] Yingpan Wu,Lixin Yu, Lidong Lan, Haiyang Zhou , Beijing Microelectronics Technology Institute, China,IEEE International symposium, 2008. A coverage driven constraint random based functional verification method of memory controller.

[7] Akhilesh Kumar and Chandan Kumar,Department of E&C Engineering, NIT Jamshedpur, Jharkhand, India. IJAET 2011. Functional Coverage Analysis of Ovm Based Verification of H.264 Cavld Slice Header Decoder.

[8] Young-Nam Yun, Jae-Beom Kim, Nam-Do Kim, Infrastruct Design Center, Samsung Electron. Co. Ltd., South Korea, soc design conference, 2011. Beyond UVM for practical SoC verification.

[9] www.verificationacademy.com.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 296 - 298, 2014, ISSN: 2319–8656

Energy saving Wireless Sensor Networks using Kerberos

Upasana Bahuguna
TULA's Institute, The Engineering and Management College
Dehradun, Uttarakhand India

Anju Devi
Uttarakhand Technical University
Dehradun,Uttarakhand India

Shashi Bhusan
TULA's Institute, The Engineering and Management College
Dehradun, Uttarakhand India

Abstract: The wireless sensor network is an networking field that combines sensing, computation, and communication into a single tiny device. As sensor networks frame closer towards well-known deployment, security issues become a vital concern. So far, much work has focused on making sensor networks realistic and useful, but still security in sensor network data communication is big issue for research. This paper proposed the idea of having different Kerberos authentication architecture for the different clusters in sensor network to save energy factor of the sensor nodes and to save time for data communication between the sensor nodes in the network.

Keywords: Wireless Communication Network; Wireless sensor network; data dissemination; Kerberos authentication.

1. INTRODUCTION

The proliferations of wireless communication networks (WCN), such as mobile *ad hoc* networks (MANET), and wireless sensor networks (WSN), make their performance issues equally important, if not even more important, because a WCN is more complex in nature than the wired CN, its components are less resourceful, and the components are more susceptible to failures. Limited resources (*e.g.*, battery, memory, and bandwidth) reduce the intrinsic performance of WCN, and thus methods to improve the metrics in WCN are imperative. The node mobility in WCN makes network links have higher unavailability rates and makes the performance analysis of a WCN even more difficult.A WCN comprises a set of nodes each of which is capable of transmitting to or receiving from other nodes. The nodes in the network, among others, can be a computer, concentrator, end user terminal, mobile station, repeater acting as a transmitter/receiver, or a sensor node. Two nodes in a WCN, in contrast to a *wired* CN, are connected by wireless communication links either directly (without infrastructure – the *ad hoc* mode) or through a base station (the infrastructure mode). In an *ad hoc* WCN, the wireless nodes communicate with each other without using a fixed infrastructure, and when two nodes are not within their transmission range, the intermediate nodes relay the messages between nodes. In some networking environments, such as wireless home or office with stationary workstations, the network nodes are wireless but non–mobile (*stationary*). In others, the network nodes are both wireless and *mobile* [1]. The stationary nodes form a fix topology or a random topology (*ad hoc*), if deployed randomly. An *ad hoc* network with mobile nodes is a *mobile wireless ad hoc network* (MANET) [2]. MANET is a new frontier for WCN and is different from a traditional WCN in many ways. One major difference is that a routing path in MANET uses a sequence of *mobile* nodes, a wireless link connecting each pair of the nodes.

The *wireless sensor network* (WSN) is another class of WCN. Nodes in WSN, forming a certain topology, can be mobile or stationary and deployed randomly (*ad hoc*). Typically, a WSN comprises more but less resourceful nodes than those in the other types of WCN.Each sensor node is capable of processing a limited amount of data[3].

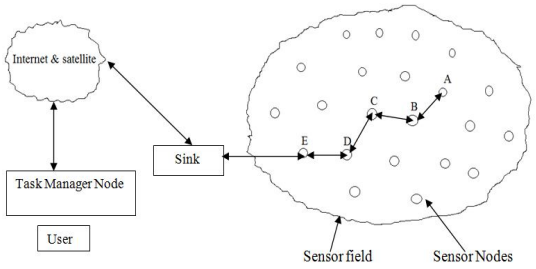


Figure 1: Communication architecture of wireless sensor networks

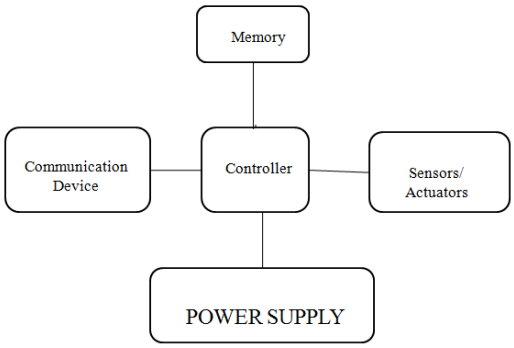


Figure 2: Sensor Node Architecture

Figure 1 and Figure 2 depicts the communication and sensor node architecture in wireless sensor network.

Earlier, the sensor networks consist of many small number of sensor nodes that were wired to a central processing station. Nowadays, the major focus is on wireless Sensing nodes. Because of the character of wireless communications, resource constraint on sensor nodes, size and density of the networks, unidentified topology prior to deployment, and high danger of physical attacks to unattended sensors, it is a confront to provide security in WSNs. The main security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages have to be authenticated [4]. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments.An opponent can use natural impairments to modify information and also render the information unavailable. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities [5].

2. RELATED WORK

Kerberos authentication scheme [4] is used for the authentication of base station in sensor network. It provides a centralized authentication server whose work is to authenticate user by providing him the ticket to grant request to the base station. Earlier proposals have provided architecturefor the authentication of base station in the wireless sensor network based on the Kerberos server authentication scheme [5].

2.1 Kerberos Architecture:

With reference to the figure below there are two main components of Kerberos server

- Authentication Server
- Ticket Granting Server

2.1.1 Authentication Server

The Authentication server knows the password of all the users and stores them in a centralized database. The authentication server shares a unique secret key with every server. These keys have been distributed to the user using a security mechanism.

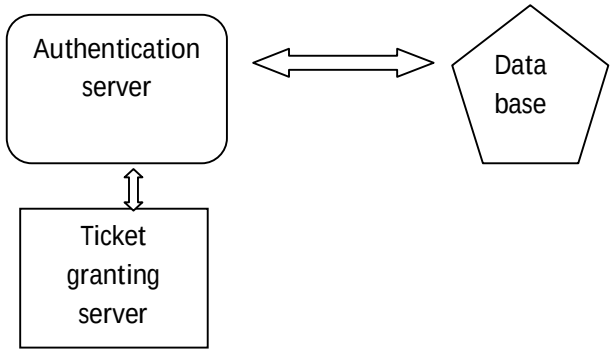


Figure 3: Kerberos Architecture

2.1.2 Ticket Granting Server

The Ticket granting server performs the work of issuing tickets to users who have been authenticated to authentication server. The first work that is to be performed is that the user first requests a ticket from the authentication server, then this ticket is saved by the user. Each time the user authenticate itself, the ticket granting server grants a ticket for the particular server/Base Station. The user save each of the service granting ticket and uses it to authenticate to a server whenever a particular service is requested.

2.2 Loopholes in earlier proposed research work:

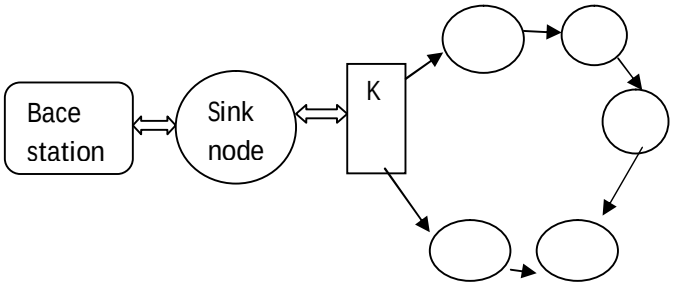


Figure 4: Sensor network with a single Kerberos

The major loopholes in earlier sensor networks were that each node in a wireless sensor networkhad only a single authentication centre i.e. the Kerberos. Due to this, all the sensor nodes had to wait for a long time for their authentication and to establish connection with the sink node and the base station. The major disadvantage of this technique of communication was that each node suffered from energy loss with the wastage of time. There was a need to overcome this problem and check the efficient solutions for it.

3. PROPOSED TECHNIQUE

This paper proposes a solution for the above mentioned problem. Instead of serving one sensor node at a time with the same Kerberos center, clusters of sensor nodes in a wireless sensor network can be formed, each having its own authentication centre for authenticated process i.e. the Kerberos. Here proposed solution will serve each node in the wireless sensor network by authenticating each sensor node it through the particular Kerberos of that cluster and then letting the nodes to communicate with the sink node and finally to the base station.All over the process of proposed technique will do work to saving energy factor of sensor node .

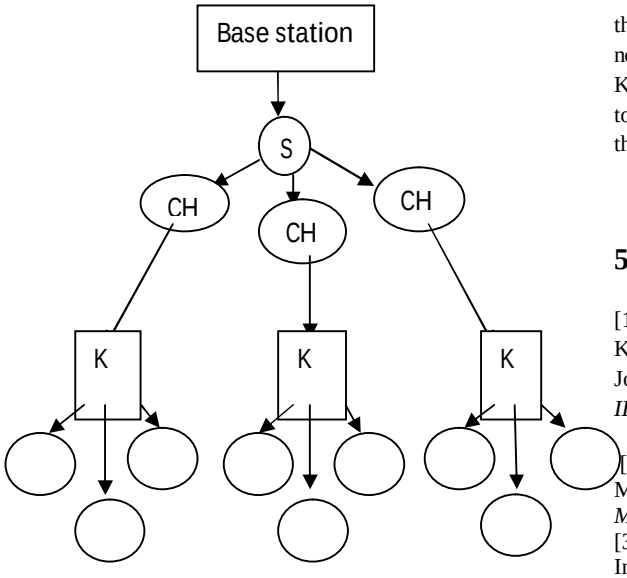


Figure 5: Clusters of sensor nodes and the sink with a kerberos

From the above figure, the proposed solution can be easily understood. Here there is more than one cluster of sensor nodes having their own authentication centre i.e. Kerberos. Each node of a cluster communicates with the authentication centre provided in the concerned cluster and then contacts to the sink node and further to the base station. This proposal will save the power of the sensor nodes and will make the communicating network efficient and reliable. The Kerberos is also present at the sink node so that whenever an intruder tries to attack the sink, the sink node carries the authentication process with the help of Kerberos and only authenticated user will be able to contact the sink node.

3.1 Advantage Of Proposed Technique:

This technique can avoid more time and heavy traffic load with less energy consumption. In traditional network when more than one node send request to the Kerberos it takes more time to response which results in processing delay and leads to loss in energy of sensor nodes in sensor network. By implementing proposed technique where different Kerberos are used for different clusters, they will process the nodes request at the same time and this will result in less processing delay as well as will save the energy of the processing nodes. Hence it will be energy efficient technique. Also, the sink node is protected from any unauthenticated user for any attack.

4. CONCLUSION

The main purpose of this paper is to provide secure data communication among sensor nodes. The proposed model uses Kerberos authentication services in clustered sensor network. This will help to detect unauthorized objects in cluster itself rather than detecting it in complete network. On implementing Kerberos technique in every cluster will save the time as well as will improve the lifetime of the sensor nodes in wireless sensor network. Also, implementing Kerberos near sink node, will allow only authenticated users to contact it. Future work will include the implementation of this proposed technique in every possible scenario.

5. REFRENCES

[1] J. Kohl, B. Neuman and T. Ts'o The Evolution of the Kerberos Authentication Service, in Brazier, F., and Johansen, *D.Distributed Open System Los Alamitos, CA: IEEE Computer Society Press*, 1994

[2] S. Jiang, N. Vaidya, and Wei Zhao, Dynamic Mix Method in Wireless Ad Hoc Networks. *In Proc. IEEE Milcom*, Oct 2001

[3] C. Shen, C. Srisathapornphat, and C. Jaikaeo, Sensor Information Networking Architecture and Applications,*IEEE Pers. Commun.*, Aug. 2001, pp. 52–59.

[4] Kurose JF and Ross KW, Computer networking, a top-down approach featuring the internet, *third edition.Addison Wesley*, Reading, MA,2005.

[5] Gupta, M. Millard, S. Fung, Y. Zhu, N. Gura, H. Eberle and S. C. Shantz - Sizzle: A standards-based end-to-end security architecture for the embedded internet, in Third IEEE International Conference on Pervasive Computing and Communication (PerCom 2005), Kauai, March 2005

[6] M. Cardei, Shuhui Yang, and Jie Wu, "Fault-Tolerant Topology Control for Heterogeneous Wireless Sensor Networks," *Proc. Of IEEE International Conference on Mobile Ad hoc and Sensor Systems*, Florida Atlantic Univ., USA, pp. 1-9, October 2007.

[7] K. Lu et al., A Framework for a Distributed Key Management Schemein Heterogeneous Wireless Sensor Networks, *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, Feb. 2008, pp. 639-647.

[8]Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, Security Issues in Wireless Sensor Networks, *international journal of communications*Issue 1, Volume 2, 2008

[9] Qasim Siddique, Kerberos Authentication in Wiireless Sensor Networks, *Annals. Computer Science Series. 8th Tome 1st Fasc*,2010.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 299 - 303, 2014, ISSN: 2319–8656

Remote Control based Audio-Video Content Filter Application for Philips 2K10 TV with JointSPACE Architecture

Mohan Kumar J
School of Information Sciences
Manipal University, Manipal.
India

Sandhesh Gowda
School of Information Sciences
Manipal University, Manipal.
India

Rahul Devi Reddy
School of Information Sciences
Manipal University, Manipal.
India

Harishchandra Hebbar
School of Information Sciences
Manipal University, Manipal.
India

Sundaresan C
School of Information Sciences
Manipal University, Manipal.
India

Chaitanya C.V.S
School of Information Sciences
Manipal University, Manipal.
India

Abstract: JointSPACE is an Open Source project that allows every user/supplier to develop applications for Philips TV displays. JointSPACE is based on the SPACE architecture which was developed by Philips to ease internal development. At a certain point of time, Philips decided to open its architecture to allow everyone developing code for the TV target. In this paper we propose and implement a Remote control application for Audio-Video Content Filter Application. One of the major issues with people watching the Television shows, as a family with children, especially in Asian context, there may be some inappropriate visuals with audio may appear. These contents affect the children mental health. So a remote application is created to mask the video and mute the audio for the required time, by the user. Even the change of channel may have the similar type of content. So this application is not providing the complete solution for this problem, but helps in certain scenarios.

Keywords: Philips JointSPACE TV, Directfb, Voodoo, Mobile Applications

1. INTRODUCTION

Television (TV) is an essential entertainment media in common man's life. Presently smartTv started emerging and in the next decade, the user space will be more. These smart TV run a particular software platform for running the applications. One such software platform is JointSPACE from Philips. JointSPACE is an Open Source project that will allow every user/supplier to develop applications for Philips TV displays. JointSPACE is based on the SPACE architecture which was developed by Philips to ease internal development. At a certain point of time, Philips decided to open its architecture to allow everyone developing code for the TV target. [1][2].

2. JointSPACE

JointSPACE facilitates mainly 2 aspects:

i. Integration of applications made by suppliers.

ii. Integration of applications made by customers. JointSPACE addresses this by opening and extending the current TV architecture. [1]

Some of the features of Jointspace are:

JointSPACE proposes a single platform to develop applications. The platform may be any Linux PC or device capable of running Linux/DirectFB technologies. JointSPACE publishes the essential TV APIs used in the SPACE architecture. JointSPACE provides portable prototyping software that includes and illustrate the essential of the SPACE architecture. [1]

JointSPACE extends the TV architecture to allow:

1. Executing TV applications on a remote system, rendering and being controlled on the TV
2. Executing application on a remote system, controlling the TV APIs remotely [1]

JointSPACE continuously provide new technologies/libraries to ease and improve the development of new applications. JointSPACE extends the TV API to allow controlling more TV functionalities. As JointSPACE is based on DirectFB technologies; following DirectFB packages are used

- DirectFB 1.4
- SaWMan 1.4
- FusionDale 0.8.1.

The JointSPACE exposes 3 core APIs apart from these packages for developers, as shown in Figure 1.

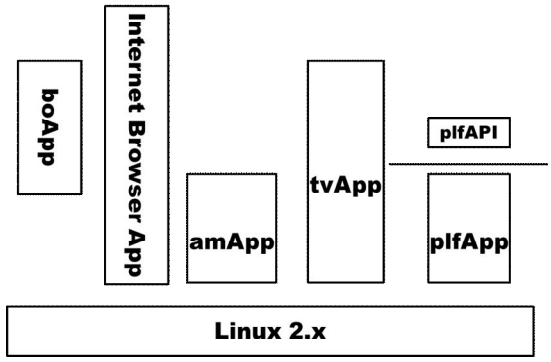


Figure 1. JointSPACE Architecture

plfApi is the API for control various platform devices, like Audio/video setup and playback, demux, tuner control,

Picture and sound properties (Brightness, contrast, volume etc.)

plfApi is the key API which needs to be explicitly managed because multiple application will need to access it. To reduce complexity of resource management plfApi is divided into a number of resource groups

- Source
- Front End
- Audio featuring
- Video Featuring
- Connectivity
- Mute

2.1 Resource Management – plfApi

Management of plfApi is done by application manager (amApp).All applications needing to control any of plfApi interfaces must create these special windows of directfb and use the window Id as an identifier to call plfApi.Audio node window for calling plfApi functions related to audio control. Border window for calling any other plfApi functions.

All plfApi calls are routed through a resource gating layer within the plfApp which only allows calls with the owned window ID. Application request resource groups of plfApi that they need to call towards amApp. AmApp ensures that the requesting application's window ID is set into resource gate of plf.

2.2 Application Manager API

Application Manager API (amApi) is the API used for communication between clients and application manager.Some of the important functions available are:

- Power related functions: PreparePowerState, RequestPowerState, ConfirmPowerState.
- Platform Resources: RequestPlfApi, PlfApiDenied.
- Key grabbing: RequestKey.
- Activities: Requesting various activities.
- Focus management: RequestOverlay, SetFocus
- Multiview: AddToLayout, MoveToLayout.
- System event management: DisableEvents.

2.3 Connection Management

The connection between the remote device and the television is established by a set of processes. Firstly the application manager api, amapp, starts the communication, after the device discovery. Then the remote device calls the directfbinit function, so that the jsapp master can fork another process jsapp1. Also the process will be added to the application manager. Then the remote device initiates directfbcreate and createwindow functions. Then a window will be created inside the application manager for the particular process. Then the remote device requests requestfocus, through jsapp1 so that the application manager focuses to the amapp.

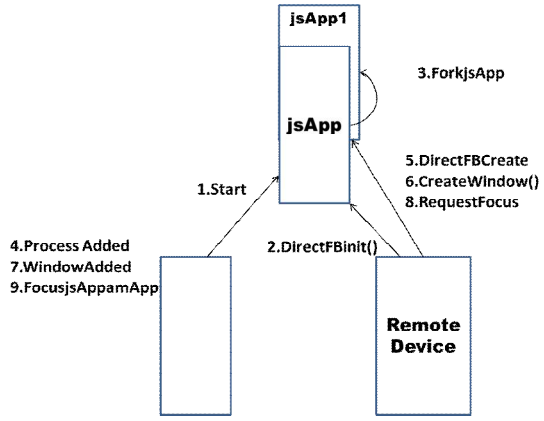


Figure 2. Connection Management

2.4 DirectFB – Direct Frame Buffer

A thin library that provides hardware graphics acceleration, input device handling and abstraction, integrated windowing system with support for translucent windows and multiple display layers, not only on top of the Linux Frame buffer Device. It is a complete hardware abstraction layer with software fallbacks for every graphics operation that is not supported by the underlying hardware. DirectFB adds graphical power to embedded systems and sets a new standard for graphics under Linux.[5]

2.5 JointSPACE Simulator

The jointSPACE simulator allows to experiment with the SPACE architecture on a Linux PC[3][4]. It is splitted into various packages organised into sub-directories.

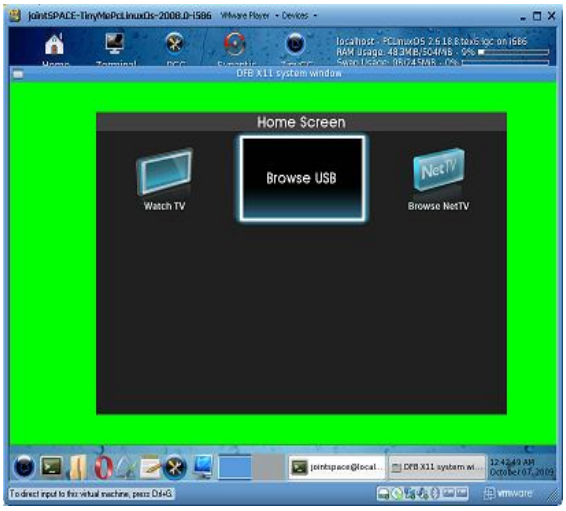


Figure 3. JointSPACE Simulator[4]

The package currently includes: DirectFB (in the form of

installation scripts and patches, as DirectFB itself is hosted at directfb.org), the basic SPACE applications (amapp, plfapp, homeapp, tvapp other examples in the form of source code), the basic libraries required by SPACE (presenting amApi and plfApi to all applications, across processes' boundary using FusionDale IPC; in the form of dynamic libraries and header files), the platform porting glue header files (papi), mainly required by HW suppliers to integrate their platform in the architecture (the default plfapp delivered is based on a papi implementation delivered in source code but mainly consisting in stubs that could be mapped on standard Linux device drivers as v4l or other higher level packages as SDL or mplayer.)

These packages represent the minimum required by the simulator. New packages will be added during the life time of this project (new libraries, new APIs etc) to ease the development of future applications.

3. REMOTE APPLICATIONS

Remote applications are applications running on external devices, making use of TV capabilities to render GFX and media. External devices can be any computing device including iPod/iPhone, game consoles, PDA, lightweight PC, PC servers, MAC. Remote applications are using the IP network (wired or wireless) to communicate with the TV. It can be used to extend TV functionality with customizable features, integrated together with "standard" TV applications. Remote applications can also be controlled with the TV remote[6]. They are making use of DirectFB/VooDoo technologies and follow (joint)SPACE architecture rules.

Two kind of remote applications are currently supported:

1. Applications to control the TV remotely (inject events like keys over the network)
2. Applications making use of the TV resources to render GFX and media content.[6]

3.1 Block Diagram

A remote based content filter application has been created for the television, which can be used at the any remote device. Here the users have to press a key in a remote device, which can be a laptop or a mobile phone, pressing the key will block the content and wait for the another key press for releasing the content. For the implementation a laptop is considered as a remote device. This can be extended to mobile phones. Instead of the Television, the JointSPACE simulator is used [2], which is an open source simulator for the Philips JointSPACE Television, to test the applications.

The filter should have an application running on the Television and also another application running on the remote device. Whenever the user send a signal from the remote device, this signal will be received TV, through the Wi-Fi Connection. Once the signal is received a screen is created on top of the visual. Also the audio is muted. The simple block diagram of the implementation is shown in Figure 3.

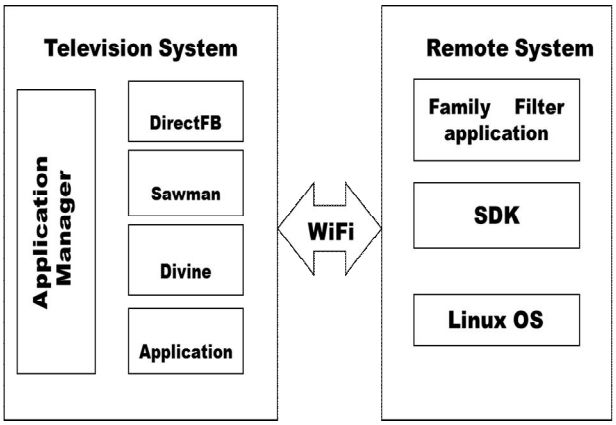


Figure 4 Block Diagram

3.2 Scenario and Scope of the Implementation

For the implementation scenario, considered certain major issues in the human life with regard to the Television. Present scenarios families face difficulty in control of children watching Television. The content broadcasted in television are sometimes not apt for children. So it is necessary to provide Parental Guidance for child. One way of avoiding is to mask the video and mute the audio, for some time. Even though change of channel can be one of the solutions, we can't predict the content broadcasted on changed channel. So this application can be used for masking video and mute audio for the required time until the user decides to unmask.

Scope of this project extends from each and every family, who is having a television, to very large display halls, where people watch different programs on television especially as a family.

3.3 Implementation

The implementation of this project was a step by step procedure. An application is created such that a signal is send from the remote device when the users press a button. A RC code is send to the TV. On the TV this code is received and accordingly a window is drawn on the video running on the TV. Also the audio is muted. The project is implemented using C programming and linux commands. Filter.c file is written when a header file Control.h is invoked. The Control.h has two functions defined, namely dfb_start() and dfb_stop(). These functions are used to input the key for masking and unmasking the video along with muting and unmuting the audio. Two threads are created, one is to show the image continuously on TV until stop event is given from the remote device. Second thread is to wait for event to stop given from the remote device ie to unmask the screen layer and unmuting the audio. The following RC code for Mute and Demute in the program which is #defined in the filter.c program.

```
#define NOTRCSOURCEMASK        0x20

#define keySourceRc6           3

#define rc6S0AvMute            163

#define rc6S0DeMute            13
```

The flowchart of the implementation is shown in Figure 5. Figure 6 shows the user input for blocking/masking the TV content. For the prototype the program waits for the user to give an input as 1.Figure 7 shows the normal TV channel watching. Once the key is pressed a new layer is created on the currently watched TV screen blocking the content. Audio is also muted. This is shown in Figure 8.

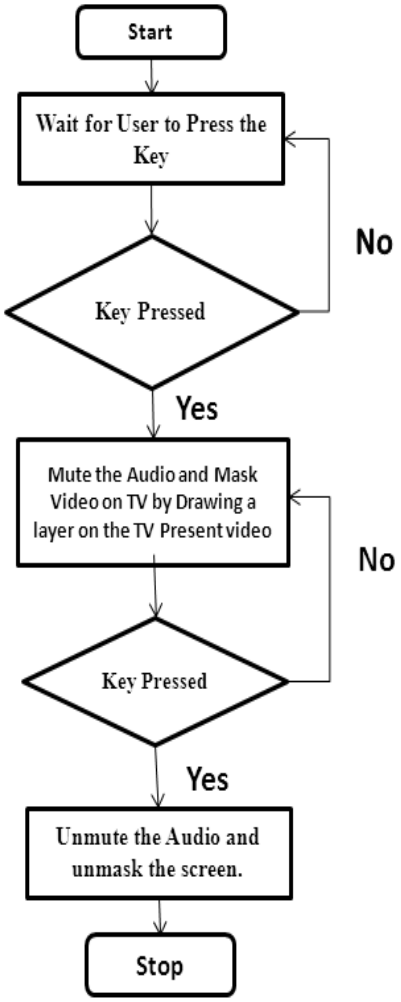


Figure 5 Flowchart of the Implementation

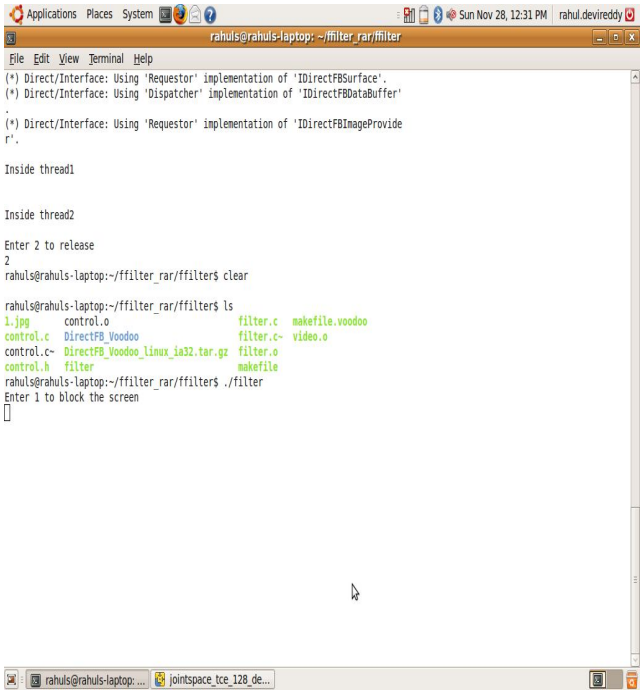


Figure 6 Running family filter application in Remote Device (laptop)

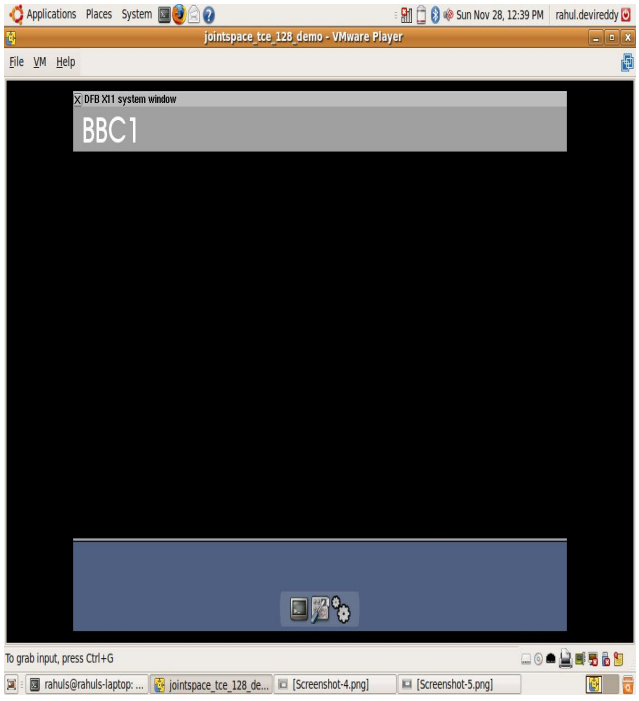


Figure 7 Watching a channel in the TV

Figure 8 Blocks the running video for a while

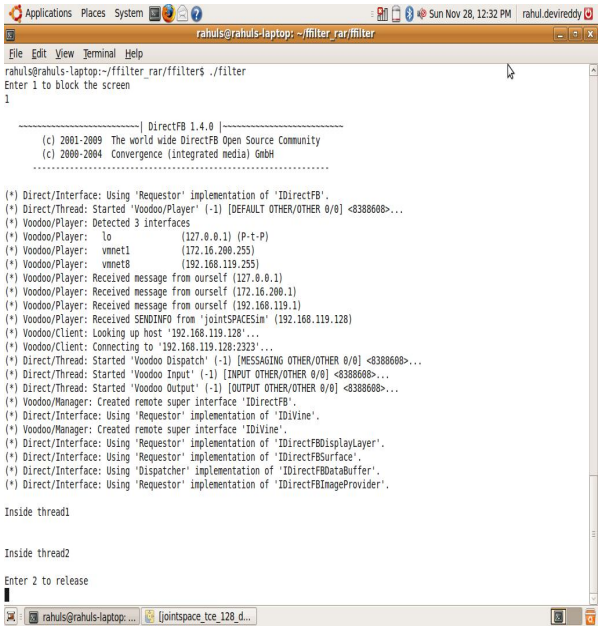


Figure 9 Sending a signal to get back to normal audio and video

To bring back the audio and video another key is pressed. Here it is number 2. This is shown in Figure 9.

4. CONCLUSION AND SCOPE

A remote based Audio-Video Content Filter Application for Philips Joint SPACE is developed and checked under the development environment. The application has the capability to block and mute the inappropriate contents when watch with the family especially with children. The application is not developed to eradicate the complete impact of problems due to watching TV by children. But it can be used in some scenarios. This application is tested on the laptop as a remote device and JointSPACE simulator. The same can be developed on an android mobile as remote control application is already available for Philips TV with JointSPACE architecture. This idea can be incorporated with the android remote control application. Similarly can be implemented for IPHONE and Windows based mobile.

5. ACKNOWLEDGEMENT

We thank Dr. A Narendranath Udupa, Philips Research, Bangalore and Mr. Manjunatha Maiya, Sr. Project Manager, MU - BoP, Philips Pvt.Ltd for providing us the JointSPACE platform training and donating a TV for executing projects.

6. REFERENCES

[1].http://foundation.webinos.org/deliverabled026target-platform-requirements-and-ipr/26-nettv-fraunhofer/ (March 2014)

[2]. http://jointspace.sourceforge.net/ (March 2014)

[3]. http://sourceforge.net/projects/jointspace/ (March 2014)

[4].http://sourceforge.net/apps/mediawiki/jointspace/index.php?title=JointSPACE_Simulator (March 2014)

[5]. http://directfb.org/ (March 2014)

[6].” System architecture for virtual world interfacing with TV platform” - Virtual world interfacing with TV platforms Article, http://wg11.sc29.org/mpeg-v/?page_id=298 (March 2014)

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 304 - 308, 2014, ISSN: 2319–8656

Data Mining: Approach Towards The Accuracy Using "Teradata"!

Shubhangi Pharande
Department of MCA
NBNSSOCS,Sinhgad Institute
Pune, Maharashtra
India

Simantini Nalawade
Department of MCA
NBNSSOCS,Sinhgad Institute
Pune, Maharashtra
India

Ajay Nalawade
Cognizant Technology Solutions
Pune, Maharashtra
India

Abstract: Data mining refers to the process or method that extracts or mines interesting knowledge or patterns from large amounts of data. Thus, the result of the natural evolution of information technology can be viewed by data mining. Data mining also involves assimilation, more willingly than a simple transformation. Data mining also have techniques from multiple directions such as database technology, statistics, machine learning, high-performance computing, pattern identification, neural networks, data revelation, information extraction as well as image and signal processing and spatial data analysis.
The large number of database systems having query and transaction processing eventually and naturally led to the need for data analysis and understanding. Hence, due to this increasing necessity data mining started its development. The process reveals hidden patterns that can't be detected using traditional query and OLAP tools. So there is "Teradata Solution", unique approach to counselling and our optimal use of data warehouse technology.[4]

Keywords: OLAP (Online Analytical Processing), pattern identification, neural networks, data revelation, machine learning, mines interesting knowledge or patterns

1. INTRODUCTION

Data mining is not a one-time event. It's a process - an ongoing evolution of discovery and analysis. It's a process that uncovers new and meaningful patterns in collected data; patterns can use to address challenging business questions that require prediction and inference. And it's a process that demands a unique set of skills and resources. Data mining also plays a crucial role in raising the value of Teradata solution. The requirements from models for prediction, estimation, and other inferences involving uncertainty are built by analyzing the huge volumes of historical data which can deliver the knowledge to take more informed strategic business decisions and more effective interactions with individual customers.[3]

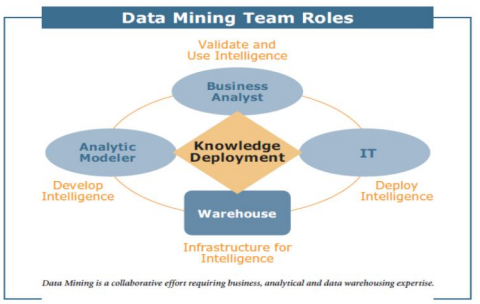


Figure 1.Data mining introduction

2. WHY DATA MINING

To transfer data into useful information and knowledge from the huge amounts of data, the concept comes in focus is “Data Mining”.

It is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations. It enables these companies to determine relationships among "internal" factors such as price, product positioning, or staff skills, and "external" factors such as economic gauge, contest, and customer demographics. And, it enables them to determine the impact on consumer regarding its sales, customer fulfillment, and corporate profits. So company can drill down huge data into summary information to provide a detail view of transactional data.

A retailer can manage current records of customer, which will help them to promote their targets which are based on an individual’s purchase history, by using data mining. Retailer can also mine demographic data which will help them to develop products & sponsorships to request for specific customer segments. For example, Blockbuster Entertainment mines its video rental history database to recommend rentals to individual customers. For example Book Library mines its rental history database to recommend rentals to individual customers.

3. DIFFICULTIES FACED BY DATA MINING

The volume and diversity of data being captured by companies today is overwhelming. To take smarter strategic decision, there is a need to turn this information into business processes and actionable plans by data analysis due to epidemic growth in collected data. The challenge or difficulty in Data Mining is to extract the exact data what you require from the enormous data collection. For e.g. the data provided by OLAP tool is three dimensional, but sometimes it happens that we don’t require un-necessarily 3rd dimension of data.

4. APPROACHES TOWARDS THE TERADATA SOLUTION

Teradata product is a product of Teradata Corporation, an American computer company that sells analytic data platforms, applications and related services. The Teradata product is referred to as a "data warehouse system" and stores and manages data. The data warehouses use a "shared nothing" architecture which means that each server node has its own memory and processing power. Storage of data can be incremented by adding more servers and nodes. Servers spread their workload with the help of database software which is present at its top. To process different types of data teradata provides its applications and software’s. In 2010, Teradata added text analytics to track unstructured data, such as word processor documents, and semi-structured data, such as spreadsheets. Teradata's product can be used for business analysis. Data warehouses can track company data, such as sales, customer preferences, product placement, etc. There is appointment for minority, women, veteran, or small business vendors due to supplier diversity program by teradata.

4.1 Teradata Master Data Manager

Master data is one of the critical parts from the database as it is going be used by business operations as well as reporting and analytics systems. There is requirement of proper master data management so that it will not put

business at risk in future. A good master data management solution mitigates that risk by managing data architecture, metadata, data quality, data hierarchies, master data workflow, and data governance. It also synchronizes master data so that changes are propagated across the entire enterprise. These all requirements can be meet by Teradata Master Data Manager and more also in a complete package which operates flawlessly with existing Teradata Solutions with lower cost than the other Master Data Management solutions from the market today.

To provide rapid analytics solution, Teradata helps us by providing data warehouse solution provider and KXEN. (A privately- held predictive analytics software vendor KXEN (pronounced as the initials K-X-E-N) is a relatively lesser - known competitor in the predictive analytics space, and has a distinct bent towards user - friendly and line – of - business predictive analysis empowerment). "KXEN's automated solutions were simple and easy to integrate, did not demand the high degree of skill and experience needed by traditional tools and team was up to speed on their use in less than two days.[5]

Rapid analytics is the practice of maximizing an existing data infrastructure and data mining technology to drive predictive intelligence into the business process. The ultimate goal is to improve the profitability of analytic projects by reducing cost and accelerating the data mining process.

Teradata provides a unique new program, Teradata® Rapid Insight Service, that's exactly what its name implies: a quick and easy low-cost way for retailers to uncover answers to some of their most pressing business questions. It's a unique combination of technology, people, and processes that can help us to become more flexible, agile, and sophisticated in our approach to solving business problems.

4.2 A Low-Risk Approach

There is a specialized team of Teradata experts that understand industry's challenges and best practices, a team that can uncover low-risk options for attacking high impact issues and identify areas in which further investment is warranted. Teradata consultants can:[6]

- Identify high impact questions, and build the business case for further analysis.
- Provide analytic results that deliver new business insight.
- Suggest actions (based on industry best practices) implied from results.
- Provide the analytical framework, models, and methodology for you to extend your own analytic expertise and resources.
- Recommend additional ways to extend analytics for further insights with data you already have.

4.3 A Low Cost Approach

Teradata Accelerate for Finance - Today's economic pressures increase the demand for quick visibility to detailed revenue and cost driver data. To enable such insights, Teradata offers a financial analytic package that leverages pre-built intelligence to turn enterprise resource planning (ERP) data into actionable information. Teradata Accelerate for Finance quickly integrates ERP data from source to end report significantly reducing the time, risk and cost of financial analytics projects. The package is designed to eliminate the usual challenges, such as limited data transparency, time consuming and costly maintenance, and disconnected financial and

operational data. This package helps companies more easily reveal economic drivers and opportunities for cost and expense reduction, for revenue growth and for improved cash flow management.[6]

5. WHY TERADATA?

5.1 Data Mining and Analytics

The volume and diversity of data being captured by companies today is staggering.[1] This exponential growth in collected data increases the demand for data analysis and the need to turn this information into business processes and actionable plans to make smarter strategic decisions.

5.2 Teradata Warehouse Miner

Teradata Warehouse Miner will help you discover meaningful new data patterns and trends. It contains an array of data profiling and mining functions ranging from data exploration and transformation to analytic model development and deployment that are performed directly in the Teradata Database. While most data mining solutions require analysts to extract data samples to build and run analytic models, Teradata Warehouse Miner allows you to analyze detailed data without data movement, streamlining the data mining process.

5.3 Features & Benefits

Teradata Warehouse Miner makes the most of your data warehousing capabilities with analytic technology that:[2]

- Reduces the analytic modeling development cycle, allowing faster iterations to refine your model and increase analytic intelligence
- Simplifies data profiling and creation of an analytic data set with built-in intelligence, complementing any data mining tool
- Allows you to quickly and easily integrate models into business applications
- Accelerates model scoring, allowing you to analyze and score data in your warehouse efficiently

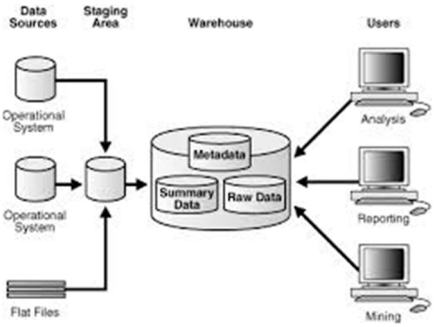


Figure 2. Working of data mining with teradata

6. CONCLUSION

By using Teradata Data Mining Services, we can mine data as well as integrate the process into our existing business procedures and technologies. The use of Data Mining makes it difficult to manage, decide and analyze the data as per the use of business. Teradata Solution focused on to explore how - and if - data mining can help our business. It's a low-risk, low-cost introduction to data mining services. We can use hardware, software and expertise - and data - to help to define a business problem, cleanse the data, develop a corresponding model and then deploy that model against our data. As a result, we get a better understanding of data mining and a clearer view of how it can benefit our business with the help of teradata solution.

7. ACKNOWLEDGMENTS

Our thanks to Prof. Tushar Dhotre, Prof.Vinay Jadhav and Mr. Sachin Pharande for their guidance in regards of this paper.

We would like to have special thanks to Dr. Smita Chavan, Associate Director of NBNSSOCS for encouraging us to write the paper and for their expert guidance.

8. REFERENCES

[1] http://www.teradata.com/business-needs/data-mining-and-analytics/

[2] http://www.teradata.com/products-and-services/teradata-warehouse-miner/?ICID=Ptwm

[3] https://www.teradata.com/.../Teradata-Data-Mining-Services-eb1719/

[4] http://www.teradatatech.com/?p=103

[5] http://decisionfirst.files.wordpress.com/2013/09/sap-acquires-kxen.pdf

[6] www.teradata.com/brochures/Teradata-Rapid-Insight-Service-eb6161/

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 309 - 311, 2014, ISSN: 2319–8656

Encrypted Query Processing Based Log Management in the Cloud for Improved Potential for Confidentiality

Nimmy Prabha
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

C.Timotta
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Tina Rajan
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Abdul Jaleef P.K
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Abstract: To address privacy concerns current implementation allows access to log records that are indirectly identified by upload-tag values. We plan to propose a practical homomorphic encryption schemes that will allow encryption of log records in such a way that the logging cloud can execute some queries on the encrypted logs without breaching confidentiality or privacy. Anonymous network implement the anonymity of users and provide privacy. In this paper implement the anonymous of user by implementing anonymous tag generation. CryptDB is a system that provides practical and provable confidentiality in the face of these attacks for applications backed by databases. It works by executing queries over encrypted data using a collection of efficient aware encryption schemes.. It greatly reduces the communication overhead between a log monitor and the logging cloud needed to answer queries on logs.

Keywords: Cloud computing, Homomorphic encryption, CryptDB, logging, privacy, k-anonymity.

1. INTRODUCTION

Logs are composed of log entries each contain information related to a specific event that has occurred within the system. Logs which contain records related to computer security. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routing log analysis is beneficial for identifying security inciden[1]t, policy violation fraudulent activity and operational problem.

Organization also need to protect the availability of their log. Many log have maximum size ,since as storing 10,000 most recent events or keeping 100 mega bytes of log data when the size limit is reached the log might over write the older data with new data or stop logging together both of which would causes of loss of log data availability. Over writing will cause the loss of old data or log, if log is important it will cause problems. Logs serve many functions with most organization such as optimizing system and network performance, recording the action of users and providing data useful for investigate malicious activity.

Log generation and storage can be complicated by several factors including a high number of log sources: inconsistent log content format and time stamp among source and increasingly large volume of log data. To keep the large volume of log data, cloud is used, because of its flexibility property[17] the size of storage area can be increased whenever needed, no over writing process occur. Clouds are large pool of easily usable and accessible virtualized resources. Cloud computing allows consumes and business to use application without institution and access their personal files at any computer with internet access. Cloud providers have a strong incentive to maintain trust and as such empty a higher level of security[8]. The log records stored in the cloud will be more secure.

2. RELATED WORK

For network wide logging protocol Syslog[2] is standard one. UDP is used for transfer of log file. The main disadvantage for the syslog is, at the time of transfer of log record, the log file is not protected. Many approaches are developed to protect the log files Based on some cryptographic protocol. The approaches are syslog are syslog pseudo, syslog ng, reliable syslog[3] and forward integrity[5]. Syslog ng [6]is the next approach after syslog. The protection of log record during the transfer can be achieved in syslog ng.

The encryption of log files by SSL. The advantages of syslog ng are not protecting the data modification at the end point. If the authentication process is implemented this issue can be overcome. In syslog sign[7] implement authentication of user. Authentication at origin and the detection of missing messages is implemented in the syslog sign. The reliability of log record can be achieved by detection of missing messages by adding two certificate block i.e. certificate block and signature block. For pseudonymising log file[9] the next approach is proposed i.e. syslog. The disadvantage of this

approach is confidentiality and integrity of log file cannot be achieved. Reliable syslog[4] provide the device authentication and protect the integrity of log message. key generation technique in the cryptographic protocol is introduced in the forward integrity protocol. Different keys are generated foe every log file.

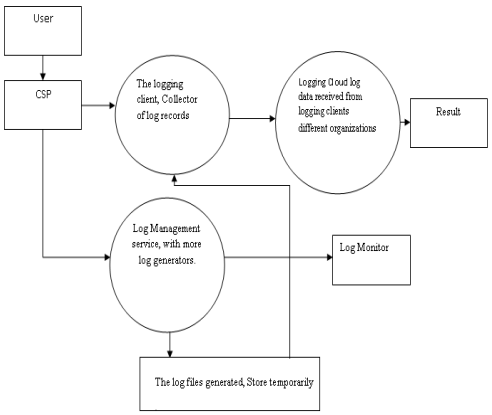
3. SYSTEM ARCHITECTURE

Cloud server: The same cloud server will store the log data from different users. The cloud service provider maintain the cloud server.

Log user: The log user receive the log record from the cloud server. The log data is transferred from the generator to the user in batches. The log user incorporate security protection on batches of accumulated log data and pushes each batch to the logging cloud.

Log generator: The temporary storage of log file in generator. The log files are divide into log batches and the encryption of log batches and key generation are take place in log generator.

Log Monitor: Log monitor generates queries to retrieve log data from cloud server. Based on the log data retrieve the log monitor performs analysis as needed. For monitor and review the log data, the function of log monitor.



The log monitor first accepts this tag and the log monitor generate another half tag then send to the cloud server. First tag generate then user upload log file to the cloud server with the help of this tag generation. The user want to retrieve the log data from cloud serve, the user should send the tag for retrieve this data.

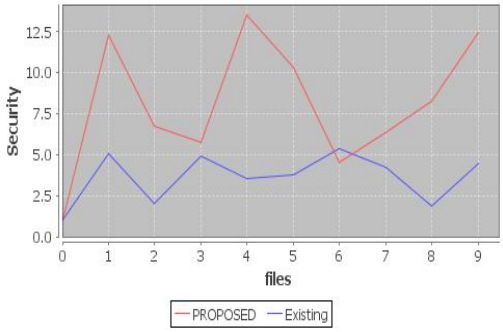
With the help of this tag cloud server or the log monitor check the user is authenticated or not. K-time Authentication protocol[21] is used here for authentication process .The cloud server contain the encrypted log data with the upload tag. The encryption of log record using different techniques.Proactive secret sharing[20] is used. During encryption public[16] and private key are the main content in the encryption.The upload tag is generated by using two half tag. One with the log monitor and user and another one with the log monitor and cloud server. So because of this the attacker attack the cloud server, they did not get details about the log data.

In a network privacy is the main concern, the solution for the privacy can be provided by anonymous communication[14][15]. he privacy in the network mean to protect from unknown spectators which causes threat to the organization. The main aim of anonymous communication in network is without releaving the organization identity, the organization can communicate with cloud for their use.

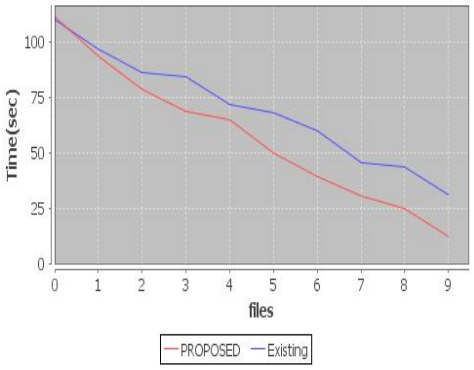
Cloud provide service to many organization or same cloud server store log data from different users. So privacy issues will occur in the cloud. By providing the anonymity[10] these can be controlled. The cloud server accepts log data only from authorized user. The user became authorized by generating an upload tag and send to the cloud server through log monitor.

4. ANALYSIS

The level of security is shown in graph. The graph shows security level of proposed system and existing system. The graph shows the security issues when adversary party get the sensitive information. The security of log files on the basis of encryption techniques[19] used in the existing system and the proposed system. In the proposed system the encryption of log file by homomorphic encryption. After evaluation of both existing and proposed system, homomorphic encryption is efficient one.



The computation time of both proposed system and existing time is show in the below graph. The protocol at the log client side starts by generating an initial set of keys[13] that are distributed to the remote shares repositories (implemented on the same machines as the log generators) to satisfy the Shamir secret sharing[17] scheme. The batch is uploaded to the cloud with appropriate upload and deletes tags included in the packet object.



5. HOMOMORPHIC ENCYPTION

The main idea in encryption technique is to conversion of plain text to cipher text. The encrypted data undergone some complex mathematical operation without compromising the encryption. Homomorphic encryption allows some mathematical operation at the time of encryption and decryption. The encryption of data occur on datas which divided into batches. While batches formed and rejoined the relationship among these batches is preserving.

In cloud computing homomorphic techniques played an important role in encryption . Selected mathematical operation is supported in partial homomorphic encryption techniques[18].This technique is independent to the number of cipher text generated. Main issue in partial homomorphic technique is: only selected mathematical operations supported. To overcome this issue fully homomorphic technique can use. In fully homomorphic techniques almost all type of mathematical operation can supported..

6. CONCLUSIONS

In proposed homomorphic encryption schemes to encrypt the log records. In that the logging cloud can execute some queries on the encrypted logs without breaching confidentiality or privacy[12]. A system that provides a practical and strong level of confidentiality in the face of two significant threats confronting database-backed applications: curious DBAs and arbitrary compromises of the application server and the DBMS. CryptDB meets its goals using three ideas: running queries efficiently over encrypted data using a novel encryption strategy, dynamically adjusting the encryption level using onions of encryption to minimize the information revealed to the untrusted DBMS server, and chaining encryption keys to user passwords in a way that allows only authorized users to gain access to encrypted data. The implementation of the logging client is loosely coupled with the operating system based logging.

7. REFERENCES

[1] K. Kent and M. Souppaya. (1992). *Guide to Computer Security Log Management, NIST Special Publication800-92*[Online].Available: http://csrc.nist-.gov/publications/nistpubs/80092/SP800-92.pdf

[2] Sarbanes-Oxley Act 2002. (2002, Sep.). *A Guide to the Sarbanes-Oxley Act* [Online]. Available: http://www.soxlaw.com.

[3] C. Lonvick, *The BSD Syslog Protocol*, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

[4]D. New and M. Rose, *Reliable Delivery for Syslog*, Request for CommentRFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.

[5] M. Bellare and B. S. Yee, "Forward integrity for secure audit logs," Dept. Comput. Sci., Univ. California, San Diego, Tech. Rep., Nov. 1997.

[6] BalaBit IT Security (2011, Sep.). *Syslog-ng—Multiplatform Syslog Server and Logging Daemon* [Online].Available: http://www.balabit.com/network-security/syslog-ng

[7] J. Kelsey, J. Callas, and A. Clemm, *Signed Syslog Messages*, Request for Comment RFC 5848, Internet Engineering Task Force, Network Working Group, May 2010.

[8] D. Ma and G. Tsudik, "A new approach to secure logging," *ACM Trans. Storage*, vol. 5, no. 1, pp. 2:1–2:21, Mar. 2009.

[9] U. Flegel, "Pseudonymizing unix log file," in *Proc. Int. Conf. Infrastruture Security*, LNCS 2437. Oct. 2002, pp. 162–179.

[10] C. Eckert and A. Pircher, "Internet anonymity: Problems and solutions,"in *Proc. 16th IFIP TC-11 Int. Conf. Inform. Security*, 2001, pp. 35–50 .

[11] M. Rose, *The Blocks Extensible Exchange Protocol Core*, Request for Comment RFC 3080, Internet Engineering Task Force, Network Working Group, Mar. 2001.

[12] B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," *ACM Trans. Inform. Syst. Security*, vol. 2, no. 2, pp. 159– 176, May 1999.

[13] J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in *Proc. 4th Australasian Inform. Security Workshop*, 2006, pp. 203–211.

[14] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proc. 12th Ann. USENIX Security Symp.*, Aug. 2004, pp. 21–21

[15] The Tor Project, Inc. (2011, Sep.) *Tor: Anonymity Online* [Online]. Available: http://www.torproject.org

[16] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inform. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[17] Rajiv R Bhadari and Nithin Mishra"Encrypted IT Auditing and Log Management on Cloud Computing" IJCSI,Vol 8,Issue No:1,September 2011.

[18] G. R. Blakley, "Safeguarding crypRtographic keys," in *Proc. Nat. ComputConf.*, Jun. 1979, p. 313.

[19] Sashank Dara "Cryptographic Challenges for computational Privacy in public clouds",CISCO system India pvt Ltd, 2011.

[20] Simarajeet Kaur" Cryptography and Encryption in Cloud Computing"VSRD_IJCS, vol2(3)242-245.

[21] I. Teranishi, J. Furukawa, and K. Sako, "*k*-times anonymous authentication (extended abstract)," in*Proc 10th Int. Conf. Theor. Appl. Cryptology InforSecurity*, LNCS 3329. 2004, pp. 308–322.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 312 - 317, 2014, ISSN: 2319–8656

Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography

Geetha G
Dept. of Electronics and Communication
BNM Institute of Technology
Bangalore, India

Padmaja Jain
Dept. of Electronics and Communication
BNM Institute of Technology
Bangalore, India

Abstract: Elliptic Curve Cryptography (ECC) gained a lot of attention in industry. The key attraction of ECC over RSA is that it offers equal security even for smaller bit size, thus reducing the processing complexity. ECC Encryption and Decryption methods can only perform encrypt and decrypt operations on the curve but not on the message. This paper presents a fast mapping method based on matrix approach for ECC, which offers high security for the encrypted message. First, the alphabetic message is mapped on to the points on an elliptic curve. Later encode those points using Elgamal encryption method with the use of a non-singular matrix. And the encoded message can be decrypted by Elgamal decryption technique and to get back the original message, the matrix obtained from decoding is multiplied with the inverse of non-singular matrix. The coding is done using Verilog. The design is simulated and synthesized using FPGA.

Keywords: Cryptography; Elliptic Curve; Finite Field; Mapping; Non-singular matrix; Elgamal Encryption; Elgamal Decryption

1. INTRODUCTION

With the rapid development of technology, people find various methods to hack information. For secured data communication, Cryptography is one of the techniques. It basically deals with encryption and decryption of a given data.

The two types of cryptography being Public and Private key cryptography, where in two types of keys are used in former and a single key is used in later case. The advantage of public key cryptography is that it is more secure than private key cryptography. ECC is one such method of public key cryptography along with RSA. The key attraction of ECC over RSA is that it offers equal security even for smaller bit size, thus reducing the band width, processing complexity [1]. In ECC, the operations such as point inverse, point addition, point subtraction, scalar multiplication are performed on the points obtained from an elliptic curve. These point operations are useful in performing encryption and decryption operations.

In paper [2], Static (One to One) and dynamic (One to N) mapping methods are explained. In static, though it is a simple technique, the same alphanumeric characters from the different words are always mapped onto the same x-y coordinates of the elliptic curve points. When encrypted, points obtained will also be same. So, an intruder can easily interpret data with trial and error method. Hence the secrecy of data transmission by using this methodology is very low. In dynamic mapping, the alphanumeric characters are mapped dynamically on to the points of EC. Thus it is difficult for an intruder to guess which particular character is mapped to which point on EC. But mapping method using matrix method as in paper [3], guarantees the security for the data. And no intruder can hack it. Since this method avoids the regularity in the resultant encrypted text. Thus strengthens the crypto systems and provides better performance.

This paper is organized as follows. The brief introduction to cryptography is given in section 1, cryptography using elliptic curves followed by the point operations, encryption and decryption operations is given in section 2, section 3 describes the proposed method, and the mapping technique followed by illustration and results in section 4, section 5 is about the future enhancements, section 6 gives conclusion and section 7 is about the acknowledgement followed by references.

2. CRYTOGRAPHY USING ELLIPTIC CURVES

2.1. Elliptic Curve

In elliptic curve cryptography, a restricted form of elliptic curve defined over a finite field F_p is considered. One particular interest for cryptography is referred to elliptic group mod p, where p is prime number. Eq.1 defines the condition for choosing the elliptic curve.

$$4a^3+27b^2 \pmod p \neq 0 \quad (1)$$

Where 'a' and 'b' are two nonnegative integers less than p. Then $E_p(a, b)$ indicates the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p. Eq. 2 refers to the general form of elliptic curve.

$$y^2=x^3+ax+b \quad (2)$$

2.2. Modular Arithmetic

Modular arithmetic is the principal mathematical concept in Cryptography. Here for every operation, modulus is taken w.r.t the prime number. Eg: Prime number considered in this work is 31.

2.3. ECC Point Operations

2.3.1. Point Inverse

If $J = (x, y) \in E(F_p)$, then $(x, y) + (x, -y) = \infty$. The point $(x, -y) \in E(F_p)$ and is called the inverse of J.

Given a point $J(x_1, y_1)$ on an elliptic curve, $-J(x_1, y_1)$ represents its inverse. The inverse of a given point can be computed using Eq. 3.

$$-J(x_1, y_1) = J(x_1, p- y_1) \quad (3)$$

Fig.1 shows the graphical representation of point inverse.

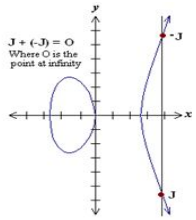


Fig.1. Point Inverse operation on elliptic curve

2.3.2. Point Addition

The Addition operator is defined over E (F_p) and it can be seen that E (F_p) forms an abelian group under addition.

The addition operation in E (F_p) is given by Eq.4.

$$J + \infty = \infty + J = J, \forall J \in E(F_p) \quad (4)$$

If $J = (x_1, y_1) \in E(F_p)$ and $K = (x_2, y_2) \in E(F_p)$ and $J \neq K$, then $L = J + K = (x_3, y_3) \in E(F_p)$.

Given two points on an elliptic curve, $J(x_1, y_1)$ and $K(x_2, y_2)$, then the addition of those points results in $L(x_3, y_3)$ which lies on the same curve. The graphical representation of point addition is shown in Fig.2. It is computed using Eq. 5, Eq. 6 and Eq. 7 as given in [4] and [5].

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \quad (5)$$

$$x_3 = \lambda^2 - x_1 - x \quad (6)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (7)$$

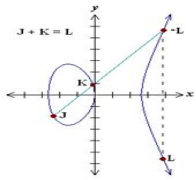


Fig.2. Point addition operation on elliptic curve

2.3.3. Point Doubling

If $J = (x_1, y_1) \in E(F_p)$, then $L = 2J = (x_3, y_3) \in E(F_p)$. Let $J(x_1, y_1)$ be a point on the elliptic curve, then point doubling yields $L(x_3, y_3)$ which lies on that curve. The graphical representation of point doubling is shown in Fig. 3. It is computed using Eq.8, Eq.9 and Eq.10 as given in [4] and [5].

$$\lambda = (3x_1^2 + a) / (2y_1) \quad (8)$$

$$x_3 = \lambda^2 - 2x_1 \quad (9)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (10)$$

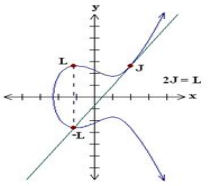


Fig.3. Point doubling operation on elliptic curve

2.3.4. Scalar Multiplication

Given a point $P(x_1, y_1)$ on the curve, to find $k^* P(x_1, y_1)$, where k is any integer, it needs repeated computations of point additions and point doublings.

The reason for choosing prime fields is that distinct additive and multiplicative inverses exist for each number i.e. 0 to (P-1) in the field of the prime number P.

2.4. ECC encryption and decryption

Let E be an elliptic curve defined over a finite field F_p. Now map the plain text on to the points Pm on an elliptic curve. Then the matrix mapping is used for higher security. Later, these points are encrypted which again represents the points on the curve. Then decryption operation is performed.

Elgamal method of encryption consists of following steps:

Step 1: Receiver selects a random integer k, and computes the point kP ('k' remains secret).

Step 2: Sender selects a random integer l, and sends the pair of points, (lP, Q+l (kP)) to receiver, here P refers to the generator point.

Step 3: To decrypt the message, receiver finds k(lP) from the first part of the pair, later subtracts it from the second part to get, Q + l(kP) - k(lP) = Q + lkP - klP = Q.

Step 4: Reverse the mapping to get back the original data sent in terms of level I mapped points.

3. PROPOSED METHOD

3.1 To obtain points on an elliptic curve

The elliptic curve $y^2 = (x^3 + x + 13) \bmod 31$ is employed in this work. i.e. by choosing a=1, b=13 and p=31in the general form of elliptic curve given in Eg.2.

The following steps are used to find out the points on an elliptic curve

Step1: Compute $y^2 \bmod 31$ for y= 0 to 31.

Step 2: For x= 0 to 31, compute $y^2 = (x^3 + x + 13) \bmod 31$.

Step 3: Match the value of y^2 in step 2 with that in step 1.

Step 4: If match is found, then the corresponding x and y becomes a point on an elliptic curve.

Step 5: For any point on an elliptic curve, its inverse will also be present.

For the above curve choosen, 34 points can be obtained including point at ∞. Here, the group is said to be cyclic, since the points repeat after 34 points.

The Table 1 gives the set of points on an elliptic curve. Let P be the generator point of the group. Now, the preliminary mapping is performed. I.e. the alphabet in the given message is mapped initially on to the points on an elliptic curve. Thus the alphabet 'a' can be mapped as P = (9, 10), 'b' can be mapped as 2P = (18, 29), 'c' can be mapped as 3P = (23, 19), and so on. Finally the alphabet 'z' can be mapped as 26P = (24, 2). Remaining 8 points can be used for mapping special characters or numbers.

Table 1: A set of points on EC

(9,10)	(18,29)	(23,19)	(4,22)	(25,16)
(17,18)	(6,24)	(24,29)	(16,8)	(20,2)
(22,22)	(28,13)	(27,10)	(26,21)	(5,9)
(19,3)	(10,0)	(19,28)	(5,22)	(26,10)
(27,21)	(28,18)	(22,9)	(20,29)	(16,23)
(24,2)	(6,7)	(17,13)	(25,15)	(4,9)
(23,12)	(18,2)	(9,21)	∞	

3.2. Matrix mapping methodology

In this section, a mapping method based on matrices is discussed. The alphabetic characters are mapped on to the points on an elliptic curve. Here, both the sender and receiver agree upon few common relationships among them.

Some of the parameters are defined as follows:-

$E(F_p)$: The set of points on an elliptic curve.

P: Generator point of the curve with order N.

S: Set of the mapping points generated by the proposed algorithm.

A: Non singular matrix, i.e. |A| ± 1 which has only integer entries.
A^{-1}: Inverse of matrix A.
l: Senders private key.
k: Receivers private key.

The following steps are given for matrix mapping method:-
Step 1: Transform the alphabetic characters into points on elliptic curve.
$[P_1(x_1,y_1), P_2(x_2,y_2),\ldots\ldots\ldots, P_n(x_n,y_n)]$
Let m be the original message of length n. If n is divided by 3, then the points have to be padded with ∞, which represents space.
Step 2: Create the matrix of 3*r with entries as points on EC. Here, take r =n/3 and s = 2n/3. The matrix M is given as

$$\begin{bmatrix} P1 & P2 & P3 & \ldots & Pr \\ Pr+1 & Pr+2 & Pr+3 & \ldots & Ps \\ Ps+1 & Ps+2 & Ps+3 & \ldots & Pn \end{bmatrix}$$

Step 3: A non singular matrix of 3*3 such that |A| ±1 is selected. Using addition and doubling of points, find Q = AM.
Where, matrix A is given as

$$\begin{bmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{bmatrix}$$

Step 4: The result is set of points S.

$$S = [Q_1(x_1,y_1), Q_2(x_2,y_2),\ldots\ldots\ldots, Q_n(x_n,y_n)]$$

4. ILLUSTRATION AND RESULTS

Choosing non-singular matrix A as

$$\begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

Then, the inverse matrix of A is given by

$$\begin{bmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{bmatrix}$$

Let sender's private key l be 25 and receiver's private key k be 13. Now Q = AM yields matrix mapping points, Encrypted points as (C_1, C2) = (lP, Q+l(kP)), Decrypted points D as (C_2-kC_1). The original message can be obtained from decrypted points (D) using the formula $M = A^{-1}D$.

4.1. Simulation results using Xilinx

The coding is done in Verilog with Xilinx ISE 13.2 simulator. Fig.4 shows the simulation set up.

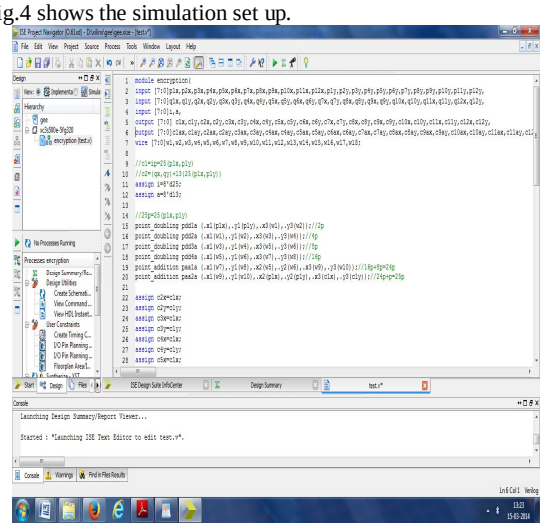


Fig.4. Simulation set up

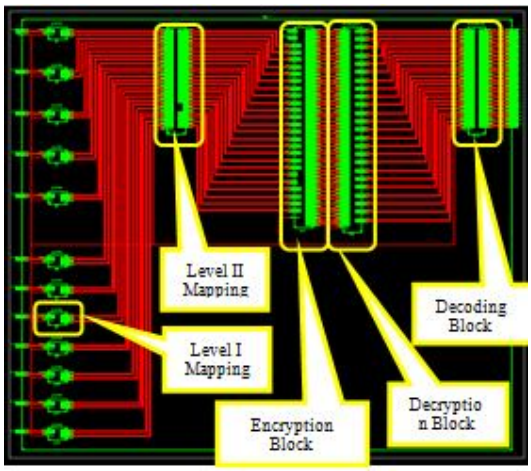


Fig.5. RTL schematic of ECC Top module

The Fig. 5 gives the RTL schematic of the Top module consisting of level I, level II mappings, encryption, decryption along with decoding.

4.1.1. Addressing letters by its ASCII values

The letters in the given word are addressed by its ASCII values. For the example word "experimenter", level I mapping block is given by Fig.6 with its ASCII values shown in Fig.7 and Fig.8 shows the level I mapping is as discussed in Table 1.

Fig.6. Level I mapping block.

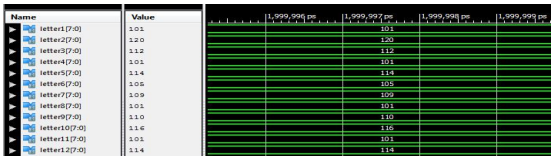


Fig.7. Showing the ASCII values for the word "experimenter"

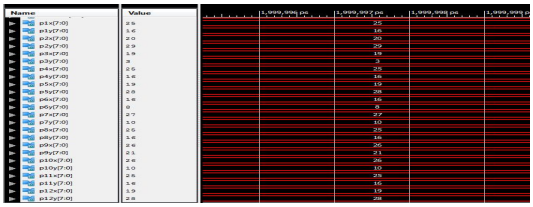


Fig.8. Respective points for the letters in the chosen word on an elliptic curve

4.1.2. Basic point operations

4.1.2.1. Point Inverse

The point inverse of a point say J = (9, 10) is given by L = (9, 31-10) = (9, 21). Here Fig.9 shows the RTL schematic of Point Inverse and Fig.10 gives its simulation waveform.

Fig.9. Block diagram of Point Inverse operation

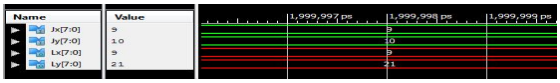


Fig.10. Point Inverse operation on elliptic curve

4.1.2.2. Point Addition

The point addition of two points say J= (16, 8) and K= (19, 28) yields $x_3 = 6$ and $y_3 = 7$. Fig.11 shows the RTL schematic of point addition and Fig.12 gives its simulation waveform

Fig.11. Block diagram of Point addition operation

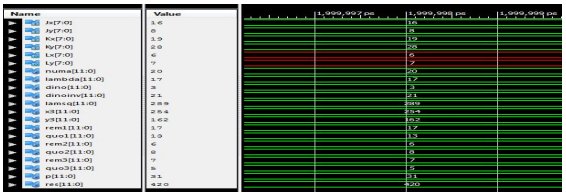


Fig.12. Point addition operation on elliptic curve

4.1.2.3. Point Doubling

When a point is doubled say J = (18, 29) yields $x_3 = 4$ and $y_3 = 22$. Fig.13 shows the RTL schematic of point doubling and Fig.14 gives its simulation waveform.

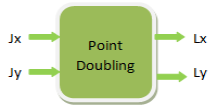


Fig.13. Block diagram of point doubling operation

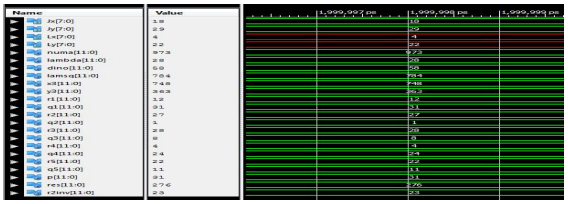


Fig.14. Point doubling operation on elliptic curve

4.1.3. Matrix mapping (level II mapping)

After preliminary mapping, the points are again mapped using matrix based mapping approach for high security. Fig.15 refers to the level II mapping block and Fig.16 refers to the matrix mapped points.

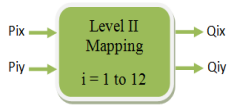


Fig.15. Level II (Matrix) mapping block

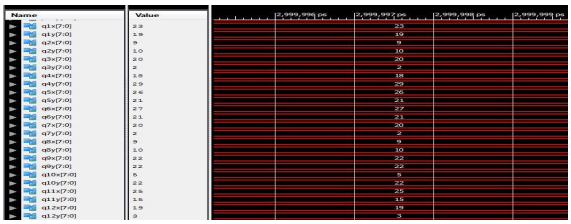


Fig.16. Matrix mapped points

4.1.4. ECC Encryption

The matrix mapped points are encrypted using the encryption formula given in section II. The Fig.17 refers to ECC encryption block and Fig.18 and Fig.19 refers to its simulation waveform of encrypted points for the example word experimenter.

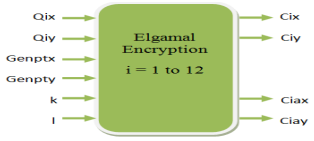


Fig.17. ECC encryption block

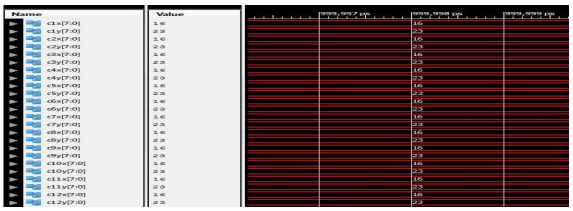


Fig.18. Encrypted points

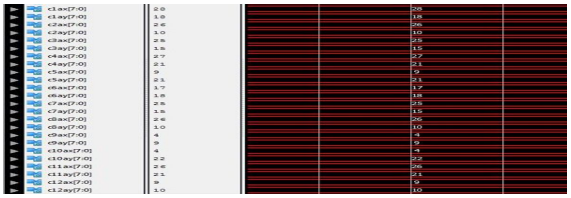


Fig.19. Encrypted points

4.1.5. ECC Decryption

The encrypted points are decrypted using the decryption formula discussed in section II. Fig.20 shows the decryption block and Fig.21 refers to the simulation waveform of decrypted points.

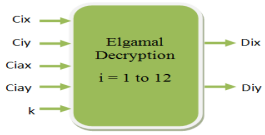


Fig.20. ECC decryption block

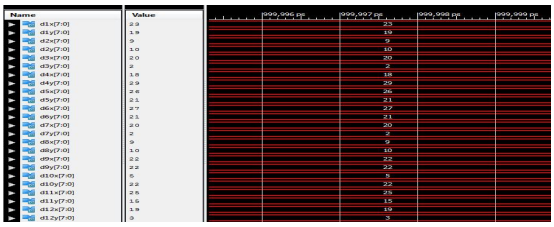


Fig.21. Decrypted points

4.1.6. Decoding

After decryption, the original message can be obtained using the formula given in section IV. Fig.22 shows the block diagram of decoding part and Fig. 23 shows the simulation waveform for the same.

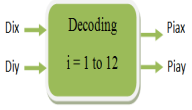


Fig.22. Decoding block

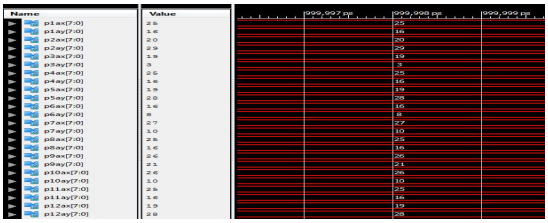


Fig.23. Decoded points

4.2. Results from CADENCE

The design is analysed using Cadence tool. Fig 24 refers to the ECC block, Fig 25 shows level I mapping, Fig 26 gives level II or matrix mapping block, followed by encryption block in Fig 27, decryption block in Fig 28 and Fig 29 refers to the decoding block, point addition block is given by Fig 30 and point doubling block is given by Fig 31.

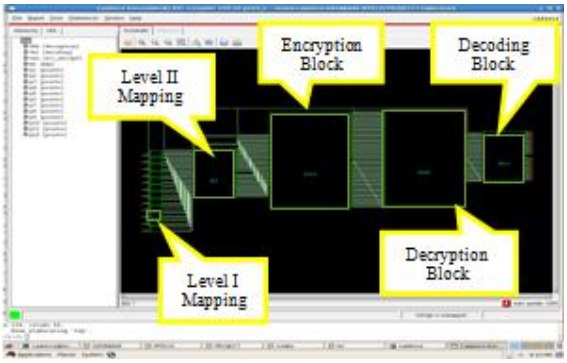


Fig.24. ECC Block using cadence

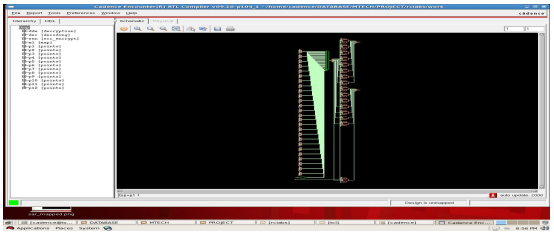


Fig.25. Level I mapping using Cadence

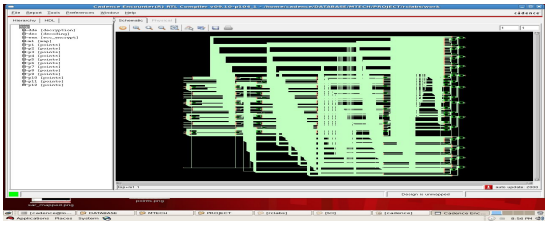


Fig.26. Level II (Matrix) mapping using Cadence

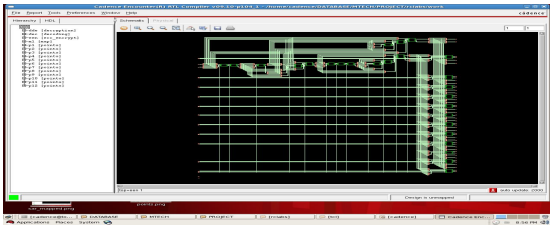


Fig.27.ECC Encryption using Cadence

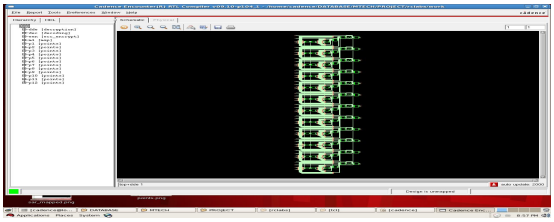


Fig.28.ECC Decryption using Cadence

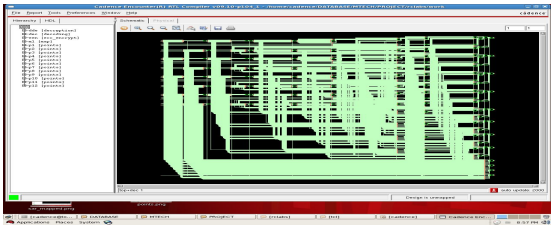


Fig.29.ECC Decoding using Cadence

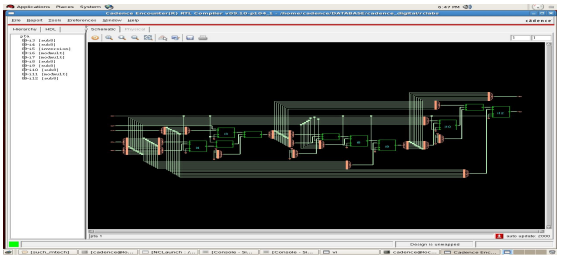


Fig.30.Point addition using Cadence

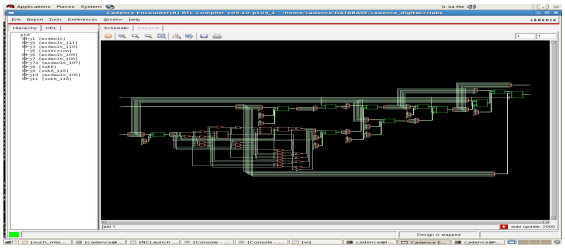


Fig.31.Point doubling using Cadence

4.3. Analysis

In Table 2, the number of point additions, point doublings and point inverses are given for respective blocks.

Table 2: Number of PA, PD and PI's required for each block

Blocks	Point Addition (PA)	Point Doubling (PD)	Point Inverse (PI)
Matrix mapping	40	24	12
Encryption	17	9	0
Decryption	36	36	12
Decoding	60	48	16
TOTAL	**153**	**117**	**40**

The Table 3 gives the area report for point addition and point doubling blocks using Cadence. The Table 4 gives the power report for point addition and point doubling blocks using Cadence. The Table 5 gives the power report for point addition and point doubling blocks using Cadence.

Table 3: Area report using Cadence

Instance	Cells	Cell Area	Net Area	Technology library
Point addition	1597	8755	0	Wireload
Point doubling	1692	8534	0	Wireload

Table 4: Power report using Cadence

Instance	Cells	Leakage power (nW)	Dynamic power (nW)	Technology library
Point addition	1597	27140.155	79593.237	Wireload
Point doubling	1692	25157.323	130700.945	Wireload

Table 5: Timing report using Cadence

Instance	Fan out	Load (fF)	Slew (ps)	Delay (ps)	Arrival(ps)
Point addition	15	18.8	0	+90	20520 R
Point doubling	18	23.5	0	+90	30014 R

5. FUTURE WORK

Optimizing the design in terms of Area, Power and Speed and extending the work so that the numerals, capital letters etc also can be encoded.

6. CONCLUSION

In this work, a method of mapping alphabetic characters to an elliptic curve points by using a non-singular matrix is described. The mapping points are encrypted and decrypted using ECC technique. The obtained results show that the chosen method avoids the regularity in the resultant encrypted points. The Table 6 gives the encrypted and decrypted points for the example word "experimenter".

Table 6: Encrypted and decrypted points for the word "experimenter"

. Char	Point P_m	Matrix Mapped points Q	Encrypted points (C1,C2)	Decrypted points D
e	(25,16)	(23,19)	((16,23),(28,18))	(23,19)
x	(20,29)	(9,10)	((16,23),(26,10))	(9,10)
p	(19,3)	(20,2)	((16,23),(25,15))	(20,2)
e	(25,16)	(18,29)	((16,23),(27,21))	(18,29)
r	(19,28)	(26,21)	((16,23),(9,21))	(26,21)
i	(16,8)	(27,21)	((16,23),(17,18))	(27,21)
m	(27,10)	(20,2)	((16,23),(25,15))	(20,2)
e	(25,16)	(9,10)	((16,23),(26,10))	(9,10)
n	(26,21)	(22,22)	((16,23),(4,9))	(22,22)
t	(26,10)	(5,22)	((16,23),(4,22))	(5,22)
e	(25,16)	(25,15)	((16,23),(26,21))	(25,15)
r	(19,28)	(19,3)	((16,23),(9,10))	(19,3)

In the paper [2], an intruder can easily guess the repeating letter since the mapping methods discussed shows regularity in the encrypted points. The mapping method employed in this paper does not show any regularity. Hence it would be difficult to guess the word. Thus it is concluded that the proposed mapping method can not only strengthen the crypto system but it also guarantee the confidentiality of messages hence providing better performance in this regard.

7. ACKNOWLEDGMENTS

Our thanks to the BNMIT management who have contributed towards this paper.

8. REFERENCES

[1] A Comparative Study of Public Key Cryptosystem based on ECC and RSA, Arun kumar, Dr. S.S. Tyagi, Manisha Rana, Neha Aggarwal, Pawan Bhadana, Manav Rachna International University, Faridabad, India, International Journal on Computer Science and Engineering (IJCSE), 2011.

[2] Efficient Mapping methods for Elliptic Curve Cryptosystems, O.Srinivasa Rao, Prof. S. Pallam Setty, Andhra Pradesh, India, International Journal of Engineering Science and Technology, 2010.

[3] Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, F. Amounas and E.H. El Kinani, Moulay Ismaïl University, Morocco, International Journal of Information & Network Security (IJINS), Vol.1, No.2, June 2012, pp. 54~59, ISSN: 2089-3299.

[4] William Stallings, "Cryptography and network security principles and practice" , *Prentice Hall,5th Edition, 2011*

[5] Darrel R. Hankerson, A. Menezes and A. Vanstone, "Guide to Elliptic Curve Cryptography", *Springer, 2004.*

[6] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[7] http://www.certicom.com/index.php/ecc-tutorial

[8] http://www.eccworkshop.org/Engineering,UK, 2009

International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 318 - 324, 2014, ISSN: 2319–8656

Analysis of Leaf Diseases using Learning Image Superresolution

Sanket B. Kasturiwala
SIPNA. College of Engineering and Technology, Amravati
Maharashtra, India

Siddharth A. Ladhake
SIPNA College of Engineering and Technology, Amravati
Maharashtra, India

C.U.Patil
Dr.Panjabrao Deshmukh Krushi Vidyapith,
Soybean Regional Research Center, Amravati.
Maharashtra, India

Abstract: Superresolution is a process of extracting higher details. The main objective of this paper is the study of patch based method for super-resolving low resolution of a leaf diseased image. The domain specific prior is incorporated into superresolution by the means of learning patch based estimation of missing high frequency details from infected leaf image. Images are decomposed into fixed size patches in order to deal with time and space complexity. The problem is modeled by Markov Random Field which enforces resulting images to be spatially consistent. The spatial interactions are coupled with a similarity constraint which should be established between high-resolution training image patches and low resolution observations of leaf diseased images. Through this proposed work, fine edges of SR images are preserved without applying complex mathematical algorithms based on wavelet, fast curvelet, etc. Also gives the better visual SR image as that of complex multi frame SR algorithms like reconstruction and registration. This concept is most useful for agricultural expert for helping our farmers. The experimental result shows the best visible SR result of an infected leaf along with MSE and PSNR.

Keywords: Markov Random Field, high-resolution, SR images.

1. INTRODUCTION

In agriculture, the analysis of infected leaf area is of great importance for the application of techniques such as pruning, fertilization and planting density [2]. A feature that can be extracted by analyzing the leaf area is the quantification of damage caused by pests and diseases. Such damage can be detected through the study of damaged leaf area by pests [2]. Detecting the precise amount of damaged leaf area is essential to determine control actions such as application of pesticides, since a small damaged leaf area may dispense control measures. In this paper, we have analyzed infected leaf image using learning based image superresolution techniques in order to recover the high frequency details such edges, various features, etc.

Obtaining a high-resolution (HR) image from single or multiple low-resolution (LR) images, known as "super-resolution" has been a classic problem. High resolution means high pixel density, also refered to as high-definition (HD). An HR image brings out details that would be blocked out in an LR image.

Super resolution problem is an ill-posed inverse problem. Estimating details is an inverse problem since low resolution observation is the result of a smoothing and downsampling process [3]. Basically, SR technique is broadly categorized in two parts. First is traditional image reconstruction and registration technique [5],[6] in these methods attempt to solve the problem by employing and fusing a number of low resolution images. The images are of an underlying scene are positioned into a common coordinate frame by sub-pixel shifts of images. Most of the literature available on super-resolution is for multi-frame and majority of them are based on the motion as cue. The super-resolution idea was introduced by Tsai and Hung, where a pure translation motion has been considered [1]. In such methods the quality of reconstructed SR image obtained from a set of LR images depends upon the registration accuracy of the LR images and some prior knowledge of imaging system [5, 6]. Nearly all SR reconstruction algorithms are based on the fundamental constraints that provide less useful information as the magnification factor increases also less computationally efficient to get more accuracy. Baker and Kanade found these limitations and developed a SR algorithm by modifying the prior term in cost to include the result of a set of recognition called as recognition based super-resolution or hallucination [11].

And second is single image learning based SR methods [7] which is more powerful and useful, when only a single observation image is available and several other high resolution images are present in the data set. All high resolution images from data set will act as training images. This method is classified under the motion free superresolution scheme as the new information required for predicating the HR image is obtained from a set of training images rather the subpixel shifts among low resolution observations.

This exploit the prior knowledge between the HR examples and the corresponding LR examples through the so-called learning process. Most example-based SR algorithms usually employ a dictionary composed of a large number of HR patches and their corresponding LR

patches. The input LR image is split into either overlapping or non-overlapping patches. Then, for each input LR patch, either one best-matched patch or a set of the best-matched LR patches are selected from the dictionary. The corresponding HR patches are used to reconstruct the output HR image.

In this paper, we propose a novel single image example-based super-resolution algorithm which combines the learning phase

of [7] by searching for examples within the Gaussian pyramid of the input image itself and the reconstruction phase of [7], which uses the Markov Random Field (MRF) model to reconstruct the HR image. The main benefit of such learning approach is that no external database is required which results in faster search and absence of "hallucination" effect (when compared with [7]). On the other hand, using MRF in the reconstruction enables us to stay in the example based domain without combining it with classical SR as in [8]. There are a few advantages to this in comparison with [8]. First of all, we can use only one level of the pyramid as the search space whose sub-sampling factor corresponds to the magnification factor instead of multiple levels with non-integer sub-sampling factor and, thus, again decrease the computation time. Second, we reconstruct only the HR image of the desired resolution rather than employing course-to-fine reconstruction of images at intermediate resolutions. Finally, we avoid sub-pixel registration which often causes in accurate results.

This paper achieves fast image super-resolution by reducing the size of trained dictionary. Thus, the reduced dictionary size makes it possible to significantly speed up SR processing and save the memory cost, while providing reasonable visual quality. Thus, the learning based approach is mostly advantageous over conventional reconstruction based SR approach.

2. LOW RESOLUTION IMAGING MODEL

We further assume that each of the measured image is contaminated by non-homogeneous additive Gaussian noise, uncorrelated between different measurements. Fig. 1 illustrates the image degradation model. In order to treat the most general case, it is assumed that each measurement is the result of different blur, noise, motion, and decimation parameters. Translating the above description to an analytical model, we get

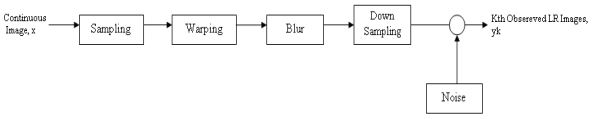


Fig. 1: Degradation Model.

$$y_k = DB_k M_k x + n_k \; for 1 \le k \le p \qquad (1)$$

The geometric warp matrix M_k is a one-to-one representation of the optic flow between the *nondecimated noiseless* version of the *kth* measured image and the ideal image x.

The assumption on the *a priori* knowledge of the blurring matrix, B_k can be explained in some applications by referring the blur to measurable phenomena, such as optics and sensor blur. In other cases, we may assume that the superresolution restoration process is robust to errors in the blurring function.

The decimation ratio between the ideal image and the *kth* measurement image can only be determined by parameter matrix D . This ratio is directly drawn from the ratio between the number of pixels in the measured image $[N_k \times N_k]$ and the ideal image $[L \times L]$ .The above restoration problem can be formulated in terms of the following equation

$$y_k = H \cdot x + n_k \; for 1 \le k \le p \; . \qquad (2)$$

Where, $H = DB_k M_k$.

3. LEARNING BASED IMAGE SUPER-RESOLUTION

We propose a single-image example-based super-resolution method which uses MRF to model the HR image as a collection of overlapping HR patches whose

Possible candidates are obtained from the input LR image itself. The algorithm can be divided in to three main phases as shown in fig. (3): learning, reconstruction and post processing.

In the learning phase, we find candidate patches of each unknown HR patch by first searching for k-nearest neighbours of its corresponding known LR patch from the input image. This search exploits the patch redundancy across different scales of the Gaussian pyramid. We then extract the HR pairs of the found neighbours (called "parent" patches) from the input image and we use them as candidate patches for corresponding locations in the HR image, because we assume that the LR and HR patches are related in the same way across different scales [12].

The next is the reconstruction phase, which models the HR image as a MRF and performs inference on this model. MRF model has a great advantage over the simpler alternative, i.e. choosing the best match at each location, as we will demonstrate shortly.

Finally, we apply post-processing techniques to eliminate remaining artifacts such as edges. We use back-projection to ensure the consistency of the HR result with the input LR image. In case of a small input image and high magnification factor, the search space may become too small for good matches to be found. This will result in visible artifacts (edges) so we also use steering kernel regression [12,14] that produces a smooth and artifact (edge)-free image while still preserving edges, ridges and blobs. Post-processing together with MRF modeling allows us to obtain competitive SR result even with only having LR image as the algorithm's input.

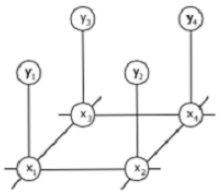


Fig. 2: RF Model : x_k – unknown HR patches;
Y_k - measured LR patches

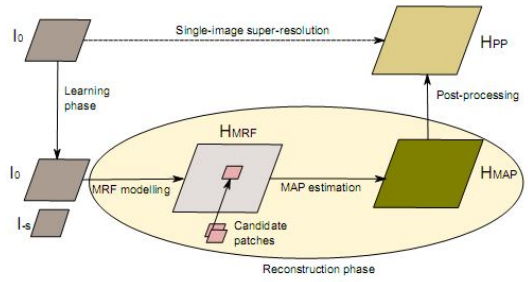


Fig. 3: Learning Based SR model.

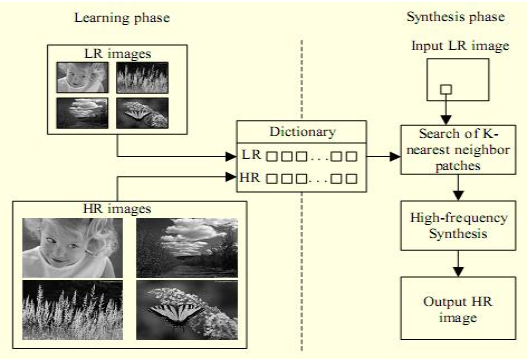


Fig. 4: HR-LR Dictionary Learning Based SR model.

As shown in fig. 4, at the learning phase, the training data, that is, a dictionary consisting of LR and HR patches, is constructed. The LR and HR patch pairs are obtained from various training images. During the synthesis phase, the input LR image is super-resolved by using the dictionary. For each LR patch in the input image, its nearest neighbor LR patches are explored from the dictionary. The high-frequency components of the input LR patch are synthesized using the best matched LR patches.

The performance of those learning-based SR algorithms highly rely on matching accuracy of an input LR patch with candidate LR patches in the dictionary. In order to improve the accuracy of matching, a sufficient number of LR-HR patch pairs must be included in the dictionary. Usually, existing learning-based SR methods require hundreds of thousands of training examples for reliable performance. However, such a dictionary size causes tremendous memory cost for storing the training samples as well as awfully large computational complexity in the matching process. In order to overcome this problem, we propose a fast learning-based SR algorithm with reduced dictionary based on k-means clustering.

3.1 Learning Based Preprocessing

Before learning preprocessing, the learned dictionary should possess various HF details lost by image degradation process and specific features to index them. The HF image I_{HF} is obtained by subtracting I_{UP} from I_H, and mid-frequency (MF) image I_{MF} stands for a high-pass filtered version of I_{UP} where, I_{MF} is employed as the features for indexing. They indicate lost HF and MF layers for predicting them, respectively.

As a result, as shown in fig. 5, we extract and store salient HR and LR patches from I_{HF} and I_{MF}, respectively. Those patches are properly overlapped with neighboring patches for local smoothness. Without loss of generality, we assume that the relationship between I_{HF} and I_{MF} is independent of the local image contrast. So, we normalize the contrasts of LR and HR patches by dividing them by the energy of the LR patch. Finally, these primitive patches including edges are chosen and they are required for the dictionary. In other words, the proposed synthesis may be applied only for the selected regions.

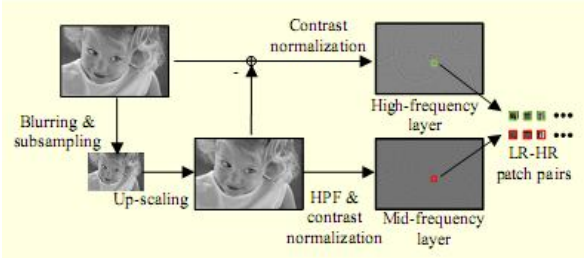


Fig. 5: Preprocessing for dictionary construction

3.2 Learning Based Dictionary Size Reduction

Now, we need to effectively reduce the number of LR-HR patch pairs in the dictionary so as to mitigate memory cost and computational burden in synthesis. This process is very significant in that the number of training examples in the dictionary generally dominates the performance of learning-based SR. Most of all, the small number of the samples can improve the practicality of the proposed SR algorithm.

So, we group adjacent LR-HR patch pairs into a single patch pair. We adopt k-means clustering to gather similar patches.

Fig. 6 illustrates this clustering process. Note that LR and HR patches in an LR-HR patch pair are always assigned into the same cluster. Finally, the center points of each cluster become new LR and HR patches belonging to the ordinary dictionary. In practice, we can determine *k* by considering memory cost and computational complexity of the synthesis phase.

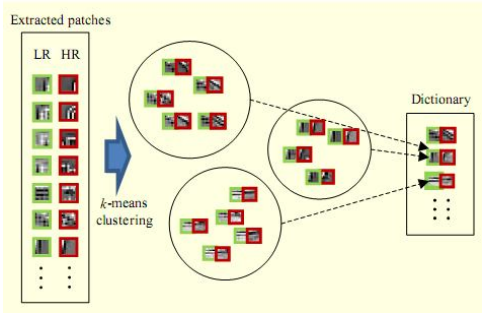


Fig. 6: Dictionary reduction using by *k*-mean clustering

3.3 Learning Based Image Synthesis

Fig. 7 describes the synthesis of learning based image SR. The input LR image is initially up-scaled using a linear scaler, and then LR patches are extracted from the MF layer of the input image as in the learning phase. Each input LR patch is compared with the candidate LR patches in the dictionary to find the best match. Next, the HR patch corresponding to the best matched LR patch is denormalized by multiplying with

the energy of the input LR patch. Subsequently, a proper residue HF patch for each LR patch is explored from the residue dictionary, and the final HF patch is obtained by adding the residue patch to the best-matched HF patch selected from the ordinary dictionary. Note that the input MF residue patch, that is, the difference between the input LR patch and the best-matched LR patch, is compared with candidate MF residues in the residue dictionary. This process is applied to all the input patches. Averaging is only performed for pixels in overlapped regions. Finally, we obtain a synthesized HR image by adding the HF image I'_{HF} to the initially up-scaled image I_{UP}.

Note that the proposed algorithm selects the single best-matched patch unlike the conventional learning-based SR algorithms using multiple nearest patches. The single best-matched patch of the proposed algorithm may correspond to the average of multiple nearest neighbor patches because adjacent LR/HR patches on Euclidean space are clustered in the training phase of the proposed algorithm.

Therefore, even though we use a single best-matched patch for HF synthesis, we can obtain a similar results to synthesis using multiple nearest neighbor patches.

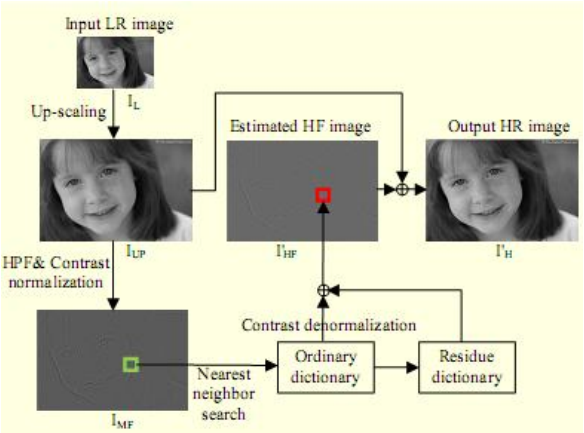


Fig. 7: Synthesis Phase

4. Mathematical Analysis

Mathematical analysis of SR is basically based on accurate MAP estimation [4]. According to the MAP estimator, the additive noise, the measurements, and the ideal image are all assumed stochastic signals. The MAP estimation of the unknown image *X* is done by maximizing the conditional probability density function of the ideal image given the measurements *P{X/Y}* . Based on Bayes rule, maximizing *P{X/Y}* is equivalent to maximizing the function *P{Y/X}P{X}* .

Bayesian approach provides a flexible and convenient way to model a priori knowledge concerning solution

X= arg max $P(x|y_1, y_2, \ldots\ldots, y_p)$

X= arg max $\{\ln P(x|y_1, y_2, \ldots\ldots, y_p) + \ln P(X)\}$

The mathematical operation shows the final result as:

$$R = \hat{X} \cdot P$$

Where,

$$R = Q^{-1} + \sum_{k=1}^{p} H_k^T W_k H_k$$

and

$$P = \sum_{k=1}^{p} H_k^T W_k Y_k$$

If we assume that the measurements additive noise is zero mean Gaussian random process with auto-correlation matrix *W* with autocorrelation matrix *Q* for unique estimate image $\hat{X}$ using iterative technique.

By considering the stochastic least mean square filtering operation in order to minimize the error function as

$$e^2 = \min E\left\{\left[f(x,y) - \hat{f}(x,y)\right]^2\right\} \quad (10)$$

The solution can be achieved through following expression

$$\hat{F}(u,v) = \left[\frac{1}{H(u,v)} \frac{|H(u,v)|^2}{|H(u,v)|^2 + S_\eta(u,v)/S_f(u,v)}\right] G(u,v) \quad (11)$$

Where, the ratio $S_\eta(u,v)/S_f(u,v)$ is called the *noise-to-signal* power ratio. For inverse filtering action it is equal to zero and $|H(u,v)|^2$ is the product of complex conjugate of $H(u,v)$ and self $H(u,v)$.

The analytical parameter such as MSE and PSNR can be calculated as, let, $x_{i,j}$ be the original image and $x'_{i,j}$ be the SR frame whose dimensions are M x N.

In this case, it is 500 x500,

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{i,j} - x'_{i,j}\right)^2$$

$$PSNR = 10 \log \frac{255^2}{MSE} dB$$

The MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) shows the better analytical result as that of conventional SR interpolation methods.

Table I shows the improved performance of proposed patch based method over conventional SR methods in terms of visual assessment parameters MSE and PSNR.

5. Experimental Analysis

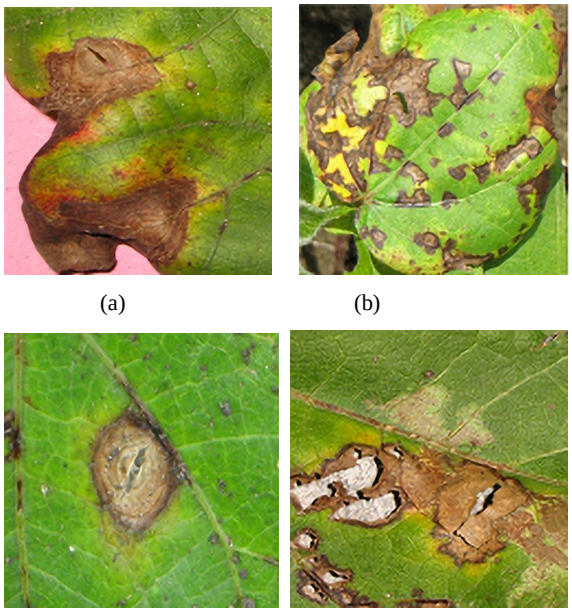
The experiments were executed on an Intel Core TM 2 duo CPU @ 2.5 GHz with 3 GB RAM and results are obtained using MATLAB 7.10 tool.

Low resolution images are captured by using a low cost LG mobile camera with resolution 125 x 125 which is pre-setted. Initially, we had captured all possible high resolution infected leaf images from surveying various farm fields in order to prepare a huge database i.e. dictionary.

In fig.8, we have taken a sample four test disease infected low resolution [125x125] leaf images for processing. Fig.9 (a) ,(b),(c),(d) shows the super-resolved high resolution images of the same of fig.8 (a),(b),(c),(d) with improved resolution of factor of 4, i. e. [500x500]

(a) (b) (c) (d)

Fig.8 Low resolution leaf diseased images [125x125].

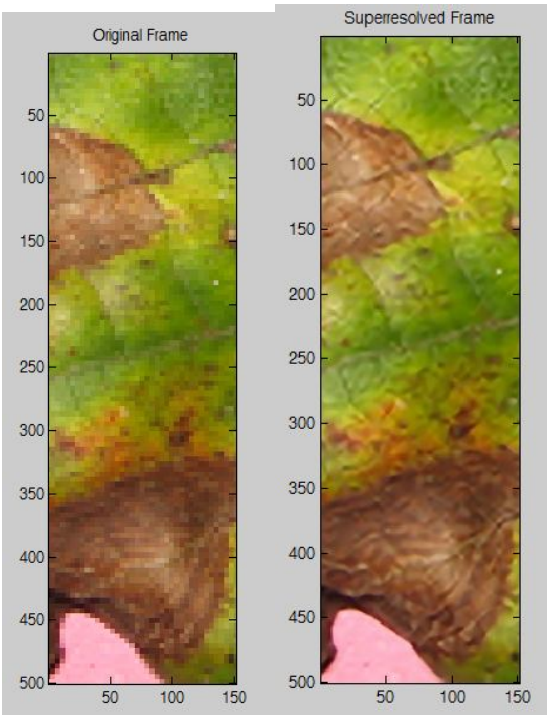


(a) (b)

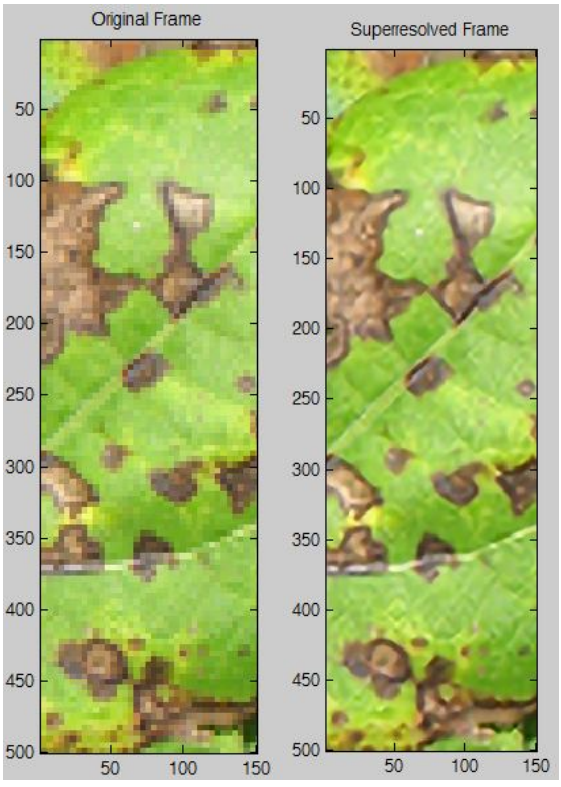
(c) (d)

Fig.9 R images of above LR leaf diseased images [500x500] with factor of 4.

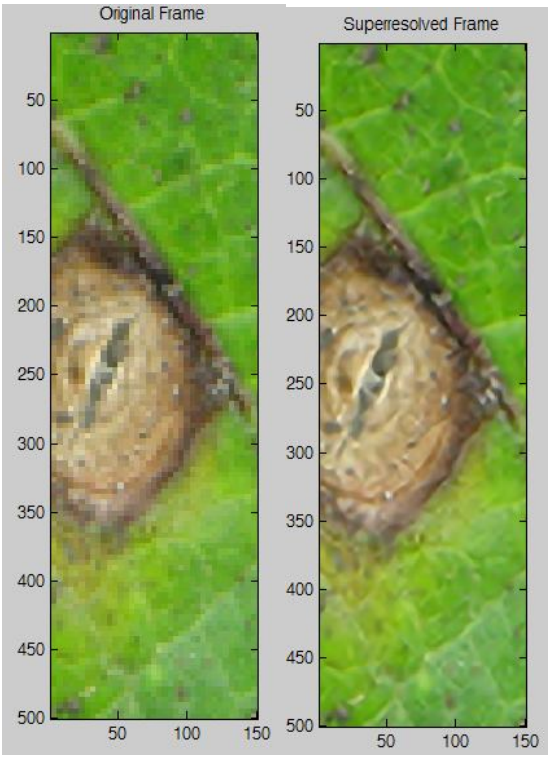
Fig. 10 shows the comparison of super fine edge quality of original frame with respect to SR frame of cropped portion of infected leaf. If the original leaf image get cropped, edge information is lost as shown in each of left side image of (a), (b), (c), (d), respectively. And on the same right side, we observe that all the edge informations are restored for the further analysis. This is the main difference between conventional algorithms and this proposed one.



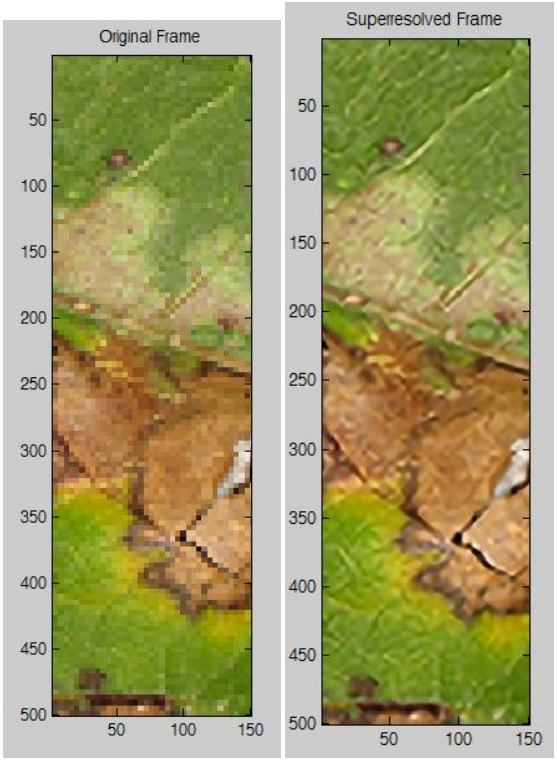
(a)



(b)



(c)



(d)

Fig.10 Comparison of Super fine edges between original image and SR image

Diseases	MSE		PSNR, dB	
	Convent.	*Proposed*	*Convent..*	*Proposed*
Disease 1	0.092	0.0020	33.13	34.94
Disease 2	0.049	0.0053	28.35	30.88
Disease 3	0.023	0.0015	32.67	36.31
Disease 4	0.044	0.0073	28.44	29.30

Table : Comparison of MSE and Psnr Between conventional Methods and proposed Method.

6. Conclusion and Future Scope

From the observational result, it is verified that the disease infected single LR image with low cost camera is only sufficient to improve its resolution with better visual quality. Information from leaf edges are recovered successfully. The proposed algorithm is very much fast with reduced size of database due to *k*-means clustering, hence memory requirement is low. Patch based learning SR technique gives improved MSE and PSNR over analytical as well as appearance result.

Properly analyzed infected leaf images are mostly useful for plant pathologist for the following purposes:

1) Identification of diseased leaf, stem, fruit ;

2) Identification and quantification of affected area by disease;

3) Identification of intensity of diseases and their effect on productivity.

Our proposed methodology is the best option for costly and complex hyper spectral satellite imagery system.

This paper will definitely bring some smile on farmer's face for improvement is crop production and agricultural development through agricultural experts.

In future, this concept can be extended to different plant pathologist for solve various agricultural engineering problems. There is a great scope for doing further research on the creation of self-learning database for any kinds of single image SR. Also, the work should be independent from the interpolating factor.

7. ACKNOWLEDGMENTS

The proposed research work is carried out under the research lab of Sipna College of Engineering & Technology, Amravati-Maharashtra-INDIA. I am also very much thank to Dr. Panjabrao Krishi Vidyapith, Regional Research Center, Amravati for kindly supporting by providing leaf images for testing as well as for preparation of a huge database.

8. REFERENCES

[1] R.Y. Tsai and T.S. Huang, "Multiframe image restoration and registration," in Advances in Computer Vision and Image Processing, vol.1, chapter7, pp.317–339, JAI Press, Greenwich, USA, 1984.

[2] Jaymala Patil, Rajkumar, "Adavances in Image Processing for Detection of Plant Diseases", Journal of Advanced Bioinformatics Applications and Research, Vol 2, Issue 2, June-2011, pp 135-141.

[3] S. C. Park, M. K. Park, and M. G. Kang, "Super-resolution image reconstruction -a technical overview", IEEE Signal Process. Magazine, vol. 20, pp. 21-36, May 2003.

[4] H.Shen, L.Zhang, B.Huang, and P.Li, "A map approach for joint motion estimation, segmentation, and super-resolution," IEEE Trans. Image Process., vol.16, no.2, pp.479–490, Feb.2007,

[5] P. Cheeseman, B. Kanefsky, R. Kraft, and J. Stutz, "Super-resolved surface reconstruction from multiple images". Technical Report FIA-94-12, NASA Ames, 1994.

[6] M. Elad and A. Feuer, "Super-resolution reconstruction of image sequences", IEEE Trans. on Pattern Analysis and Machine Intelligence, 21(9):817 1999.

[7] Kim,K.I., Kim,D.H., Kim,J.H.: "Example-based learning for image super-resolution" In: Proc. the third Tsinghua–KAIST Joint Workshop on Pattern Recognition, pp.140{148(2004)

[8] F. Sroubek, G. Cristobal and J. Flusser, "Simultaneous super-resolution and blind deconvolution", 4th AIP International Conference and the 1st Congress of the IPIA IOP Publishing Journal of Physics: Conference Series 124 (2008) 012048.

[9] Julien Mairal, Michael Elad, and Guillermo Sapiro, Senior Member, IEEE , "Sparse Representation for Color Image Restoration", IEEE Trans. on Image Proces. vol. 17, no. 1, Jan., 2008.

[10] S.Farsiu, D. Robinson, M. Elad, and P. Milanfar, "Advances and challenges in super-resolution", International Journal of Imaging Systems and Technology, vol. 14, pp. 47-57, 2004.

[11] S. Baker and T. Kanade, "Limits on super-resolution and how to break them", In Proceedings of CVPR 00, pp. 372-379, 2000.

[12] Takeda,S.Farsiu,andP.Milanfar,"Kernel regression for image processing and reconstruction," IEEE Transactions on Image Processing, vol.16,no.2, pp.349–366,2007.

[13] M.V.Afonso, J.M.Bioucas-Dias, and M.A.T.Figueiredo,"Fast image recovery using variable splitting and constrained optimization," IEEE Transactions on Image Processing, vol.19,no.9,pp.2345–2356,2010.

[14] Tijana Ru zi,HiQ.Luong, ,and Wilfried Philips, "Single Image Example-Based Super-Resolution Using Cross-Scale Patch Matching and Markov Random Field Modelling", Ghent University,TELIN-IPI-IBBT.

[15] C.H.Bock and G.H.Poole , Plant disease severity estimate visually and by Hyper spectral imaging, Plant Science, 2010 pp.59-107.

[16] Tian You-wen and Wang Xiao-juan, "Analysis of leaf parameters measurement of cucumber based on image processing", World congress on software engineering, pp. 34-37, 2009.

[17] Stéphane Pelletier and Jeremy R.Cooperstock, "Preconditioning for Edge-Preserving Image SuperResolution". IEEE Transactions on Image Processing ,VOL.21,NO.1,JANUARY2012

[18] Xinbo Gao, Kaibing Zhang,Dacheng Tao and Xuelong Li, "Joint Learning for Single-Image Super-Resolution Via a Coupled Constraint", IEEE Transactions on Image Processing , VOL.21,NO.2,Feb.2012

[19] S.Chaudhuri and J.Manjunath, Motion-FreeSuper-Resolution. NewYork:Springer-Verlag,2005.

[20] W.K.Pratt. Digital Image Processing. Wiley-Interscience, 1991.

[21] Rafael C. Gonzalez, Richard E. Woods, Steven L. Eddins, Book- Digital Image Processing using MATLAB.

[22] Sonka, Hlavac and Boyle, Book- Digital Image Processing and Computer Vision.

[23] J.Yang, Image Super-Resolution via Sparse Representation [Online]. Available: http://www.ifp.illinois.edu/~jyang29/codes/.

[24] Sanket B. Kasturiwala, Dr.S.A.ladhake, "Soybean Leaf Diseased Image Superresolution using Spatial Domain Approach", International Journal on Engineering & Research Technology, (IJERT)Vol. 1(02), 2012. ISSN 2278-0181.