RELIABILITY PARAMETER ESTIMATION AND ANALYSIS FOR ELECTRICAL UPS SYSTEM

Upendra Joshi[1], Taranjeet Singh Huda[2], Sumeet Sehrawat[3]

[1, 3]EEE Department, Amity School of Engineering and Technology, Noida, (India)

[2] ECE Department, Patel College of Science and Technology, Indore, (India)

ABSTRACT

This paper mainly concentrates on reliability analysis of electrical components. The scope of reliability is not limited to any one ofthe engineering discipline as it is a multi-disciplinary subject. In this paper reliability analysis is included with probability and statistics to provide better understanding of reliability, stress and risk analysis. Also some conventional methods have been used to frame proper estimation of practical performance analysis of replaceable and repairable electronics components. Reliability is the key feature of achieving high performance of any system. This paper is useful to calculate overall performance of a reliable system in both was i.e. quantitatively and qualitatively.

Keywords: Reliability Analysis, Failure Mechanism, Risk Analysis, Estimation, Performance Analysis

I. INTRODUCTION

Reliability Engineering is the systems probability of performing adequate function for a particular operating time, under operating conditions. It is concerned at high risk conditions. The achievements of reliability are derived from reliability engineering. The integration of reliability engineering with other engineering disciplines add throughout the systems overall development. Reliability prediction provides a quantitative baseline to assess reliability engineering in various disciplines. By focussing on reliability prediction after selecting a design we can predict rate of failures and its stress analysis completely.

II. FAILURE MECHANISMS FOR ELECTRICAL DEVICES

It is usually divided into three type's i.e. electrical stress, intrinsic and extrinsic. Higher voltage level causing damage to electrical devices or due to any human error is involved in damage then it is considered as electrical stress failure. If poor manufacturing or design procedure error takes place then it is categorised as intrinsic failure. If any error in device packaging or interconnections takes place along with environmental effects on electrical devices then it is termed as extrinsic failure.

III. AVAILABILITY ANALYSIS

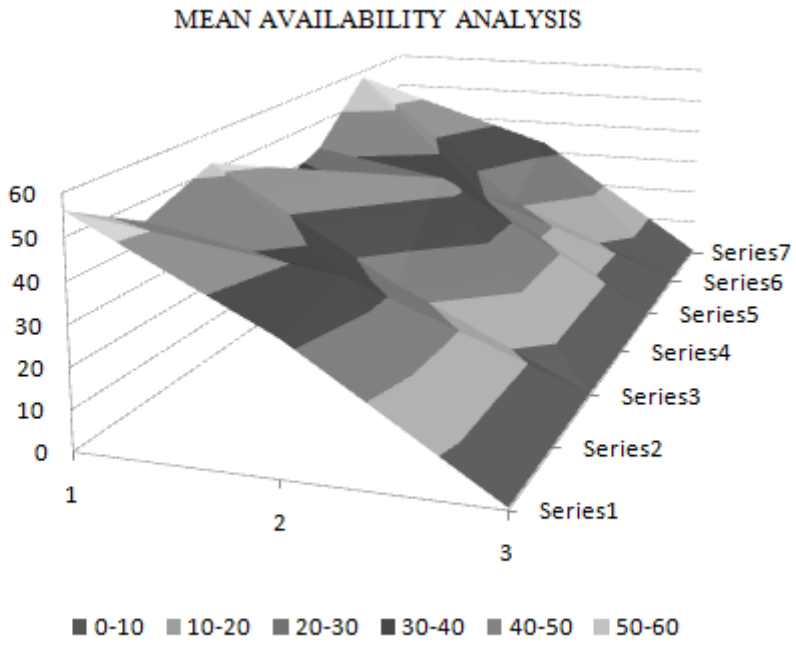
It is performed to verify operational probability of a system. Here we consider inherent availability of different system parts at operational condition during an interval of time 'T' can be expressed by,

$$A = \frac{u}{u+d} \qquad [1]$$

Where 'u' is the mean uptime during time T and d is the mean downtime during time T, T= u + d.

u	d	A
56	32	0.636364
45	36	0.555556
52	24	0.684211
36	44	0.45
42	31	0.575342
58	21	0.734177
28	33	0.459016

Table 1 Availability Data of a Power UPS System Components



Graph 1. Comparison analysis of Availability data of power UPS system components

IV. ESTIMATING PARAMETERS VIA ARRHENIUS MODEL ANALYSIS

Let us consider an electronic device to be tested under elevated temperatures of 30°C, 40°C and 50°C. Now we are assuming some data of 10 electrical components which we can take in consideration through practical performances as follows:

30°C	40 °C	50 °C
1940	605	58
3518	633	64
4593	670	82
5563	750	78
7536	1290	132
10799	1398	188
11632	1856	231
15698	2096	244
19785	2163	314
22987	2855	326

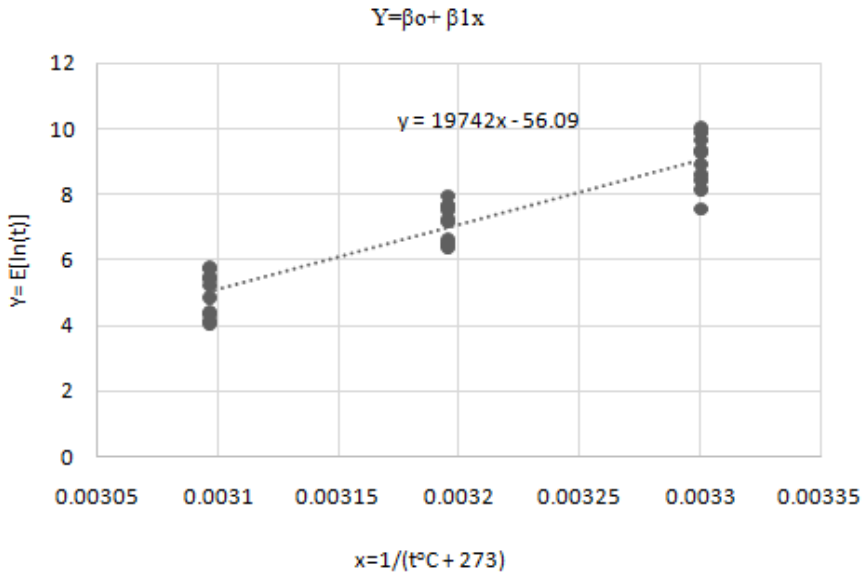
Table 2. Time to failure (t) in hours

According to Arrhenius model we have,

$$E(\ln t) = A + \frac{B}{T} \qquad [2]$$

S.no.	30°C	40 °C	50 °C
1	7.570443	6.405228	4.060443
2	8.165648	6.45047	4.158883
3	8.432289	6.507278	4.406719
4	8.623893	6.620073	4.356709
5	8.927447	7.162397	4.882802
6	9.287209	7.242798	5.236442
7	9.361515	7.526179	5.442418
8	9.661289	7.647786	5.497168
9	9.892679	7.679251	5.749393
10	10.04268	7.956827	5.786897
Σ E[ln(t)]/10	8.99651	7.119829	4.957787

Table 3. Logarithm Values of time 't' as ln (t)



Graph 2. Arrhenius model – Regression analysis graph

Using transformations Y=ln t, x=1/T, β_o=A, β_1=B we have,

Y=E[ln(t)]	t °C	x=(t °C+273)$^{-1}$
8.99651	30	0.0033
7.119829	40	0.003195
4.957787	50	0.003096

Table 4 Data Transformation of Arrhenius model

Now by using above transformed data and line equation $Y=\beta_o+\beta_1 x$ we can find estimates of parameters A and B as,

$\hat{A}=\exp(\beta 1)=\exp(-56.091) = 4.36504 * 10^{-25}\ h^{-1}$ and $\hat{B} = 19742^{o}K$ [3]

V. PROBABILITY RISK ASSESSMENT

PRA is a systematic procedure to investigate operational and building aspects of complex systems. By estimating and reducing major errors we can increase strength of any system. To analyse these errors we follow this process. Here are some major changes in this approach which have been taken place while studying this system:

1. Objectives and methodologies
2. Familiarization information
3. Logic modelling
4. Uncertainty analysis
5. Sensitivity analysis
6. Interpretation of results
7. Consequence determination

VI. CONCLUSION

Hence we have estimated parameters A and B using Arrhenius model and after analysis of Arrhenius model we can approach for risk assessment analysis and follow the above approach related to PRA. After PRA this detailed analysis can be combined with system reliability confidence limits based on component failure data. For this using Lloyed-Lipow method or Maximus method we can predict uncertainity of the system. System reliability statics via trends in observed failure events can be calculated through binomial distribution method. In future aspects we can determine Root cause analysis of the observed data and perform risk analysis of this system.

REFERENCES

[1] Reliability Engineering and Risk Analysis, A Practical Guide (CRC Press), by Modarres, Kaminskiy and Krivtsov, published 2010

[2] Military Handbook, Reliability Prediction of Electronic Equipment, Department of Defense, USA, published 2 December 1991

[3] Accelerated Testing: Statistical Models, Test Plans and Data Analyses (Wiley Series in Probability and Mathematical Statistics-Applied Probability), by Wayne Nelson, Published 1990

[4] Analysis of Failure and Survival Data, by Peter J. Smith, Published 2002

[5] Applied Life Data Analysis, by Wayne Nelson, Published 1982

[6] Applied Reliability (Second Edition) by Paul A. Tobias and David C. Trindade, Published 1995

[7] Burn-In Testing: Its Quantification and Optimization (Reliability Engineering), by Dimitri Kececioglu and Feng-Bin Sun, Published 1997

[8] Effective FMEAs: Achieving Safe, Reliable and Economical Products and Process Using Failure Mode and Effects Analysis), by Carl Carlson, Published 2012

[9] Environmental Stress Screening: Its Quantification, Optimization and Management, by Dimitri Kececioglu and Feng-Bin Sun, Published 1995

[10] Handbook of Reliability Engineering and Management, 2nd Edition, by William Grant Ireson, Clyde F. Coombs and Richard Y. Moss, Published 1995

[11] Maintainability, Availability and Operational Readiness Engineering Handbook, by Dimitri Kececioglu, Published 1995

[12] Methods for Statistical Analysis of Reliability and Life Data (Wiley Series in Probability and Mathematical Statistics), by Nancy R. Mann, Ray E. Schafer and Nozer D. Singpurwalla, Published 1974

[13] Practical Reliability Engineering, 4th Edition, by Patrick D. T. O'Connor, Published 2002

[14] Recurrent-Events Data Analysis for Product Repairs, Disease Recurrences, and Other Applications, by Wayne Nelson, Published 2003

[15] Reliability and Life Testing Handbook, Vol 1, by Dimitri Kececioglu, Published 1993

TILT DETECTOR

V. V. Mani Raghu Teja[1], S. Deepak[2], G. Anuradha[3]

[1,2,3] *Department of Electronics & Communication Engineering, B.V.R.I.T, Telangana (India)*

ABSTRACT

The Tilt Detector is used to detect the change in angular position of the system or an object and visually indicate the direction of tilt. The paper represents the total idea about this project and the working of it.

Keywords: Accelerometer, Angular Position, Arduino Uno, Direction of Tilt, Visually.

I. INTRODUCTION

Detecting the change in angular position of a system or an object is necessary for applications such as motion sensing and motion control. There must be some device which can detect that change in angular position of a system. One such device is a Tilt Detector which detects the change in tilt with the help of accelerometer.

II. TILT DETECTOR

The Tilt Detector is a device which detects the change in angular position of the system or an object and visually indicates the direction of tilt.

Figure 1: Image of a tilt detector

III. CONCEPT

An Accelerometer, which is an electromechanical device comes under the family of Micro-Electro-Mechanical Systems or MEMS devices.

Tilt detection is a simple application of an accelerometer where a change in angular position of a system or an object in any direction is detected and indicated visually through LED's. An Arduino Uno board is used to process the data received from the accelerometer and switch on the corresponding LED to indicate the direction of tilt.

IV. CIRCUIT DESIGN

The circuit only requires an Arduino Uno board, an Accelerometer module and few other components for construction.

Pins A0 to A5 of the board are connected to pins ST, Z-axis, Y-axis, X-axis, GND and VCC of the accelerometer module, respectively. The values for the accelerometer are predefined by user according to the requirement in the tilt level by using Self-Test pin (ST). Pins 8 to 12 of the board are connected to LED's.

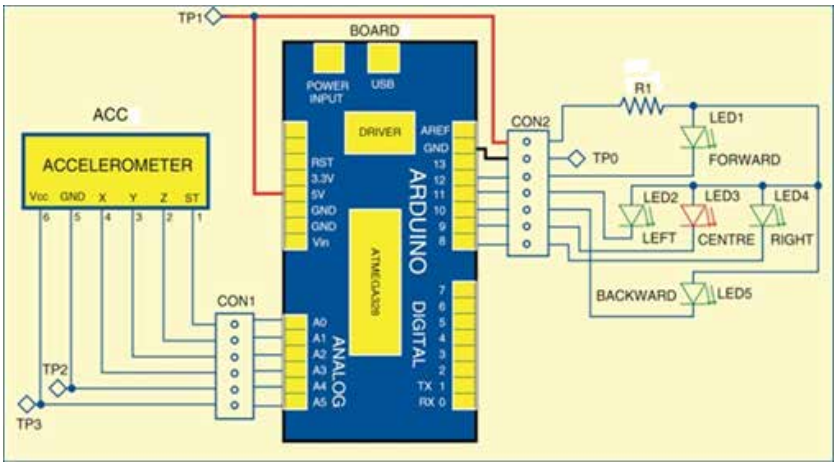


Figure 2: Circuit diagram

V. WORKING

When there is a change in angular position of the system or an object on which the accelerometer is mounted, logic levels are provided to VCC and GND of the accelerometer module through pins A5 and A4, respectively. The microcontroller of the board receives data for X, Y and Z axis from the accelerometer at pins A3, A2 and A1, respectively. This data is continuously compared with predefined values for each axis.

If the received value for any axis crosses the predefined value, the corresponding LED (Green) is lit. If the angular tilt is within the threshold limit for each direction, the LED in the center (Red) is lit.

VI. TESTING

To test the circuit, check for the voltage levels at the test points as shown in the test points table below:

Table 1: **Test points**

TEST POINTS	
Test Point	**Details**
TP0	0V, GND
TP1	5V
TP2	Low
TP3	High

For functional testing of the circuit we need to trigger the values for LED's after assembling the circuit. The steps involved in this process are:

- Connect the Arduino board to the computer with USB cable.
- Open the source code (test.ino) in the Arduino IDE and burn it on the Arduino board.

- Open the serial port from Arduino environment and press reset button.
- You will see the screen shown in Fig. 3 in which the values of X, Y, and Z axis will vary corresponding to the position of your accelerometer.

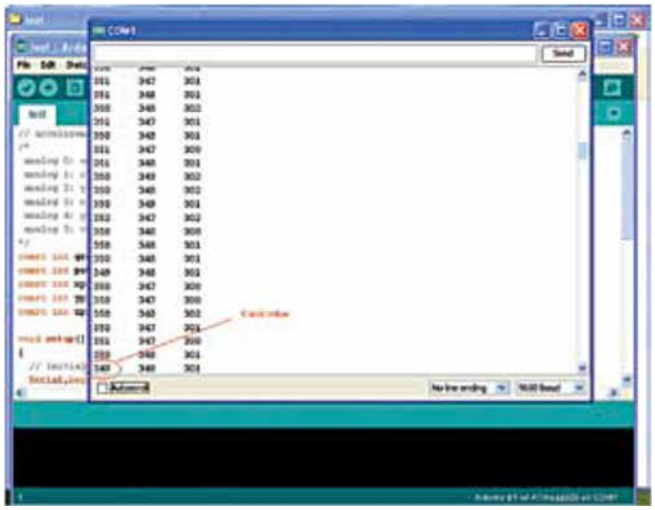


Figure 3: Screenshot of values for X, Y and Z axis

- Tilt it to the left and note the value for 'A_max' after which you want the corresponding LED to glow. The same trigger will be applied for backward tilt too.
- Tilt it to the right and note the value for 'A_min' after which you want the corresponding LED to glow. The same trigger will be applied for forward tilt too.
- The trigger values are defined by 'A_max' and 'A_min' in the final code (tiltdetection.ino).
- Open the final code in the Arduino IDE and put the values for 'A_max' and 'A_min' as shown in the Fig. 4.

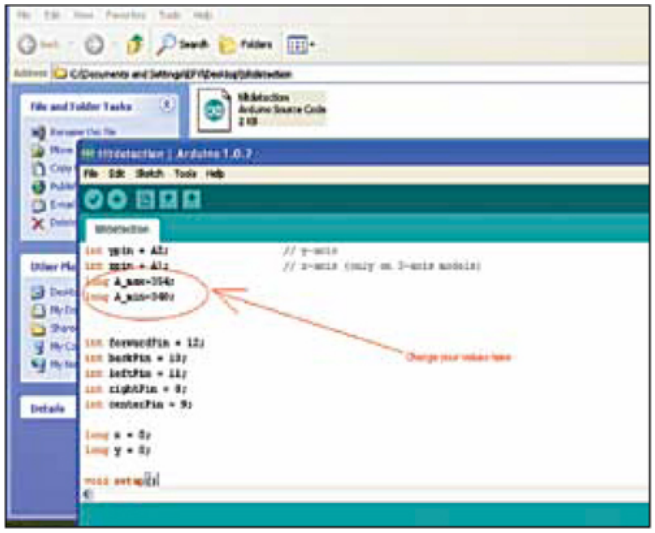


Figure 4: Screenshot of changing trigger values

- Program the Arduino again with the new code and the system is ready to work.
- If the angular tilt is within the threshold, red LED will glow. Otherwise green LED's corresponding to each direction will glow.

- You can see the same on serial port also. Connect the USB and open the serial port in Arduino environment. You will see on the serial port 'forward' if tilted forward, and similarly for the other directions.

VII. RESULTS

The results can be seen by opening the serial port in the Arduino environment as shown in the Fig. 5 below:

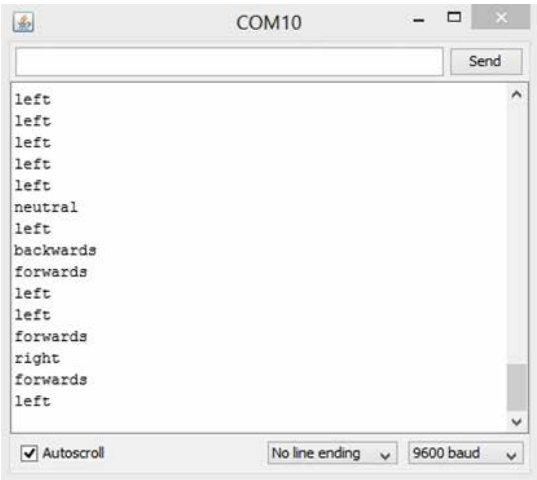


Figure 5: Screenshot of result

VIII. CONCLUSION

In summary, a Tilt Detector is a device that visually indicates the direction of tilt made by the system or an object. It can be used for various applications like tilt detection, obstacle detection, motion inputs, and earthquake sensing. It can also be used in theft protection, disk drive protection, mobile devices, gaming systems, etc.

REFERENCES

[1]. Simon Monk, *Programming Arduino: Getting Started with Sketches*, McGraw-Hill, 2012.

[2]. Accelerometer Module ADXL335, www.analog.com

[3]. Arduino Environment Guide, www.arduino.cc

[4]. Arduino Uno Rev3, www.arduino.cc

ENERGY CONSERVATION IN PNEUMATIC OPERATED FORGING INDUSTRY

[1]Jestin Francis E, [2]Dr. S Sankar

[1]M. Tech Energy Systems, Nehru College of Engineering and Research Centre, Thrissur, (India)

[2]Department of ME, Nehru College of Engineering and Research Centre, Thrissur, (India)

ABSTRACT

Forging is a manufacturing process involving the shaping of metal using localized compressive forces and the compressive force is from compressed air. An air compressor is a device that converts power into kinetic energy by compressing and pressurizing air. Air compressor unit is one of the major parts of energy consumption in most industries. Compressors are used to pressurize the air for the process requirement of the industry. In a forging industry the major part of energy consumption is by the compressor units which produces the compressed air required for powering the hammer. The compressed air is stored in tanks and then supplied to these hammering units. There is huge loss of compressed air through leakage and other faults. This would lead to a condition where the compressor units have to work for a longer time than the normal time required for producing the compressed air at required pressure. And in a forging industry different types of jobs are used and the required pressure for forging would also be different.

Keywords : Compressed Air, Forging, Hammering Units, Leakage.

I. INTRODUCTION

Energy is one of the most important factors to global prosperity. It plays a key role in achieving the desired economic growth. The entire fabric of developmental goals is webbed around a successful energy strategy. Energy is a pivotal prerequisite of developed economy and social structures. One of the major problems concerning its supply is the depleting nature of the extraction of fossil resources, combined with the need for transition to renewable energy supplies. The last depends on a number of scientific and technological breakthroughs. Meanwhile, energy conservation promises to fill the gap between supply and demand. Several measures for conservation of energy are very important for consideration. The conservation of energy, therefore, is using less more wisely than before. Saving a watt is nearly always cheaper than increasing the supply by a watt. The energy industry is one of the most capital intensive. Efficient utilization of energy resource is not only conservational it also saves capital investment. Thus conservation is really the cheapest of energy resources at least until its potential is exhausted.

About half of all energy generated in falls on industrial production. At the same time about 30% of this energy is spent by turbo mechanisms like pumps, blowers and compressors. The air compressor type, model and size are important factors in the compressor's energy consumption, but the motor power rating, control mechanisms, system design, uses and maintenance are also fundamental in determining the energy consumption of a

compressed air system. System design plays an important role in increasing the efficiency. Four aspects of system design that are crucial in deciding compressor efficiency are saving for times of need, straightening the path as narrow delivery lines, looping and sharp bends in the lines can create pressure drops in the system and reduce end use pressure, use of cooler intake air as the energy required to compress cool air is much less than that required to compress warmer air and the last one is the recovery of waste heat. It is said that for every 1 bar over the required usage pressure that a compressor generates air an extra amount of 7% will be added to the energy cost.

Over the first ten years of life of a typical air cooled compressor, with two shift operation, the operating cost (electricity and maintenance) will equal about 88% of the total lifetime cost. The cost of the original equipment and installation will account for the remaining 12%. As energy accounts for about 76% of the overall lifetime operating cost, it is very important to design more efficient components for your compressed air system. So the overall expected lifetime operating costs should also be considered, and not just the initial cost of the equipment. Most facilities can easily save 10-20% of their compressed air energy costs through routine maintenance such as the fixing of air leaks, lowering air pressure, and replacing clogged filters. Even higher savings numbers can be gained by choosing better compressor control, adding storage receiver capacity, and upgrading air dryers and filters. There is huge loss of compressed air through leakage and other faults. This would lead to a condition where the compressor units have to work for a longer time than the normal time required for producing the compressed air at required pressure.

II. FORGING INDUSTRY

Since the Industrial Revolution, forged parts are widely used in mechanisms and machines wherever a component requires high strength. Forging is a manufacturing process involving the shaping of metal using localized compressive forces. The blows are delivered with a hammer (often a power hammer). In a forging industry the first process would be the die design and die manufacture. According to the consumer demand required shape is designed on the die. Then it is taken to the forge shop where after heating the metal to a particular temperature and soaking it for a specific time in the furnace. Now shaping is done in the forge shop and then it is taken to heat treatment section and finally it is taken for finishing and testing is done as a part of quality assurance.

The hammers used here are mainly pneumatic hammers and uses compressors to provide the compressed air for its operation. The compressors are mainly reciprocating type and are run with the help of induction motors. Due to this there is large energy consumption.

III. COMPRESSED AIR

Compressed air is used widely throughout industry and is often considered the “fourth utility” at many facilities. Almost every industrial plant, from a small machine shop to an immense pulp and paper mill, has some type of compressed air system. In many cases, the compressed air system is so vital that the facility cannot operate without it. Compressed air systems consist of a supply side, which includes compressors and air treatment, and a demand side, which includes distribution and storage systems and end-use equipment. A compressor is a machine that is used to increase the pressure of a gas. A modern industrial compressed air system is composed of several major sub-systems and many sub-components. Major sub-systems include the compressor, prime mover, controls, treatment equipment and accessories, and the distribution system. The compressor is the

mechanical device that takes in ambient air and increases its pressure. The prime mover powers the compressor. Controls serve to regulate the amount of compressed air being produced. The treatment equipment removes contaminants from the compressed air, and accessories keep the system operating properly.

IV. TYPES OF AIR COMPRESSOR

A compressor is a device which is used to compress air, gas or vapour. The compressed air has wide applications in industry as well as in commercial equipment. It is commonly used in forging industry to power the hammers, in power plants for driving pneumatic tools etc.

4.1 Reciprocating air compressors

Reciprocating air compressors are positive displacement machines, means that they increase the pressure of the air by reducing its volume. This means they are taking in successive volumes of air which is confined within a closed space and elevating this air to a higher pressure. The reciprocating air compressor accomplishes this by a piston within a cylinder as the compressing and displacing element. Single-stage and two-stage reciprocating compressors are commercially available. The reciprocating air compressor is single acting when the compressing is accomplished using only one side of the piston. A compressor using both sides of the piston is considered double acting.

4.2 Rotary compressors

Rotary air compressors are positive displacement compressors. They have rotors in place of pistons and give a continuous, pulsation free discharge air. They are directly coupled to the prime mover and require lower starting torque as compared to reciprocating machine. They operate at high speed and generally provide higher throughput than reciprocating compressors. Also they require smaller foundations, vibrate less, and have a lower number of parts, which means less failure rate. The most common rotary air compressor is the single stage helical or spiral lobe oil flooded screw air compressor. These compressors consist of two rotors within a casing where the rotors compress the air internally. There are no valves.

4.3 Centrifugal compressors

The centrifugal air compressor is a dynamic compressor which depends on transfer of energy from a rotating impeller to the air. Centrifugal compressors produce high-pressure discharge by converting angular momentum imparted by the rotating impeller (dynamic displacement). In order to do this efficiently, centrifugal compressors rotate at higher speeds than the other types of compressors. These types of compressors are also designed for higher capacity because flow through the compressor is continuous. Adjusting the inlet guide vanes is the most common method to control capacity of a centrifugal compressor. By closing the guide vanes, volumetric flows and capacity are reduced. The centrifugal air compressor is an oil free compressor by design. The oil lubricated running gear is separated from the air by shaft seals and atmospheric vents.

V. COMPRESSED AIR DISTRIBUTION SYSTEMS

When a compressed air distribution system is properly designed, installed, operated and maintained, it is a major source of industrial power, possessing many inherent advantages. The primary objective of a compressed air distribution system is to transport the compressed air from its point of production to its points of use in sufficient quantity and quality and at adequate pressure for efficient operation of air tools and other pneumatic

devices. However, many other considerations come into the design of the system to ensure the efficiency and safety of the total system. These include air volume flow rate, air pressure requirements, types and number of compressors, air quality, air system efficiency, air system safety, air system layout, air volume flow rate requirements.

One problem is that the variety of points of application may require a variety of operating pressure requirements. Equipment manufacturers should be consulted to determine the pressure requirement at the machine, air tool or pneumatic device. The proper capacity to be installed is vital. The capacity rating of air compressors generally is published in terms of free air, which is at atmospheric conditions of pressure, temperature and relative humidity and not at the pressure, temperature and relative humidity required at the air tool or pneumatic device to be operated. Determination of the average air consumption is facilitated by the use of the concept of load factor. Pneumatic devices generally are operated only intermittently and often are operated at less than full load capacity. The ratio of actual air consumption to the maximum continuous full load air consumption, each measured in cubic feet per minute of free air, is known as the load factor. It is essential that the best possible determination or estimate of load factor be used in arriving at the plant capacity needed.

When a compressed air system operates at a pressure higher than required, not only more energy consumed in compressing the air, but end uses consume more air and leakage rates also increase. This increase may be referred to as Artificial Demand. To minimize the effects of artificial demand, the use of a Pressure/Flow Controller is recommended. Safety in the workplace is a primary design consideration. In a compressed air distribution system there are several factors involved. The pressure rating of all piping must meet or exceed the maximum pressure to which the system may be subjected.

VI. METHODOLOGY

Presently there are 8 compressor units and each of them run by a 270 hp motor. The compressed air distribution systemis in a ring line arrangement. There are eight storage tanks in which six of them are of 20 m^3, one of 5m^3 and one of 3m^3 and three hammers. There is large energy consumption by these compressor units. Here in the plant the compressors are operated depending upon the compressed air demand. At present the compressors are switched on or off as per the requirement of the hammers operated. This switching on and off the units leads to large energy consumption. The main drawback of the ring line arrangement it that air flow do not have a specific direction. Direction of flow is to the area of pressure drop and it changes depending upon the use of tools i.e. hammers. Sectioning of the storage tanks would be an effective method to reduce the operation time of compressors. It have been also identified that there is leakage of compressed air in the plant which demands more operation time for the compressor units.

Receiver filling method is used for the capacity testing of the compressor. Here the volume of the receiver is calculated. The sizes and the length of the pipes up to the isolation valves are measured. This volume is added to the receiver volume and called effective receiver volume. The valves which isolate the compressor receiver from the delivery lines are closed. Pressure gauge reading is noted. It reads zero as all the air in the receiver is drained. Compressor is started and kept on full load. The time taken by the compressor to reach a certain set pressure is recorded.

To estimate the amount of leakage in the system, start the compressor when there are no demands on the system. A number of measurements are taken to determine the average time to load and unload the compressor. The

compressor will load and unload because the air leaks will cause the compressor to cycle on and off as the pressure drops from air escaping through the leaks.

Total leakage (percentage) can be calculated as follows:

$$\text{Leakage (\%)} = [(T \times 100)/ (T+t)]$$

Where: T=on-load time (minutes)

t=off-load time (minutes)

Leakage will be expressed in terms of the percentage of compressor capacity lost. The percentage lost to leakage should be less than 10% in a well maintained system. Poorly maintained systems can have losses as high as 20 to 30% of air capacity and power. Leakage can be estimated in systems with other control strategies if there is a pressure gauge downstream of the receiver.

TABLE 6.1 AVERAGEPERCENTAGE ENERGY COMSUMPTION

Air compressors	33%
Forge shop equipment	17%
Die shop equipment	10%
Heat treatment equipment	17%
Canteen boiler	3%
Lighting	4%
Oil Fired Furnaces,E.O.T Cranes, Pumps, F&D equipment etc.	16%

VII. CONCLUSION

The aim of this project was to reduce the energy consumption by the pneumatic operated equipped tools in the forging industry. Due to the ring line compressed air distribution system the pattern of operation was such that all the storage tanks have to be filled even for the use of smallest rated hammer. For this minimum of three compressors have to kept in operation and at times one of them would be running in unloaded condition which is considered as leakage. So by sectioning of the storage tanks the use of compressor units could be reduced and also the energy consumption. For sectioning motorized butterfly valves are used as the overall set pressure is below 10 kg/cm^2. This reduces the need of filling all the air receivers hence reducing the unwanted operation of compressors. And by this the compressors can be operated at different pressure as the hammers require different pressure. Lower operating pressure would reduce the energy consumption.

REFERENCES

[1] WadahAljaism, “Difference between Slip Ring Motor with Conventional Drive and Squirrel Cage Motor with Variable Speed Drive”, International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue 4, April 2014.

[2] "Energy Efficiency in Air Compressors", N.C. Department of Environment and Natural Resources, Division of Pollution Prevention and Environmental Assistance, January 2004.

[3] Eric C Harding, "Energy Saving Potential by Optimising the Process of Air Generation and Consumption", Air Technology Ltd, England.

[4] "Best Practices, Technical Case Study", Office of Industrial Technologies Energy Efficiency and Renewable Energy, U.S. Department of Energy, December 2000.

[5] D.M. Glukhov, "Multiphase Induction Motors for a Variable Speed Drive", *Modern Technique and Technologies*, 2003, pp. 128-130.

[6] "Compressed Air System", Bureau of Energy Efficiency, Chapter 3, pp. 55-71.

ON THE PERFORMANCE OF CDTA BASED NOVEL ANALOG INVERSE LOW PASS FILTER USING 0.35µM CMOS PARAMETER

Aastha Sharma[1], Abhishek Kumar[2], Pawan Whig[3]

[1,2,3] *Department of Electronics and Communication,*

Rajasthan Institute of Engineering and Technology,(India)

ABSTRACT

Current Differencing Tran conductance Amplifier (CDTA) based analog inverse filter configuration is proposed in this paper. This topology can be use to synthesize inverse high pass filter (IHPF) and inverse band pass filter (IBPF). The results have been verified using PSPICE. The simulation results are closed to theoretical value.

Keywords*: *CDTA, GAIN, IHPF, IBPF, Phase

I. INTRODUCTION

Inverse filter is a building block of communication system and Instrumentation system. The inverse filters are commonly used in communication, speech processing, audio and acoustic system [1, 2] and instrumentation [3]. Inverse Filter reverse the distortion of the system that caused the distortion should be known as priori and the inverse filter i.e. used to remove distortion should have reverse transfer characteristics so as to result in an undistorted desired signal [4]. The literature survey of the inverse filter suggest that numerous type of digital inverse filter has been designed but analog inverse filter remain unexplored in this area because of limited availability of analog inverse filter circuit design [5,6]. However recent research trends that the area is now gaining a new interest. A brief literature survey to analog inverse filter is presented here. CDTA based trans-impedance type first order all pass filter has been proposed [7]. In it single CDTA with only two passive components are used. Various other digital filters are available i.e. optical focusing by spatio temporal inverse filtering of room acoustic real time inverse filter focusing through iterative time reversal and realization of current mode FTFN based inverse filter has been proposed [8]. Current mode all pass filter using CDTA has been proposed [9]. This circuit has two inputs and single output and both input provides first order all pass filter responses independently. Current mode filter and inverse filter using single FTFN has been designed. In it nuller are used for realization [10].

This literature survey reveals that a few number of analog inverse filters has been proposed so far, to the best of the authors knowledge. One analog universal filter configuration using CFOA has been proposed by Neeta Pandey [11]. Another configuration for analog inverse filter is presented here. Therefore the aim of this paper is to present analog inverse filter using CDTA. This paper gives the configuration of IHPF and IBPF.

II. CIRCUIT DESCRIPTION

Current mode technique has wide bandwidth which is virtually independent of closed loop gain, greater linearity and large dynamic range [15]. These are the key performing features of current mode technique. CDTA can operate in wide frequency range because of current mode operation and CDTA is free from parasitic input capacitance. Its input to output behavior predetermines this current component particularly for current mode. We can consider CDTA as a current operational amplifier if intermediate z terminal is not taken out .

2.1 Basic Operation

CDTA has five input nodes p, n, z, x+ and x-. It has two low impedance current input terminals p and n and an auxiliary output terminal z

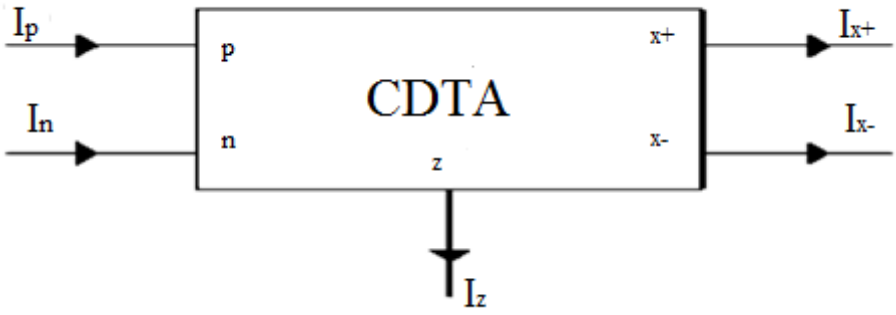


Fig.1. Symbol of CDTA

Current is applied on input terminal p and n. The difference of input current flows on output terminal z. External impedance is connected to z terminal and the voltage over this terminal is converted to the output current by the output transconductance g and provides positive output g to x+ terminal and negative output –g to x- terminal. Output current of x+ terminal and x- terminal is equal in magnitude but opposite in direction. The magnitude of current is product of transconductance and the voltage at z terminal impedance [13].

$$V_P = V_n = 0 \quad (1)$$

$$I_Z = I_P - I_n \quad (2)$$

$$I_x = g_m.V_z = g_m.Z_z.I_z \quad (3)$$

$$I_x^+ = g_m.V_z \quad (4)$$

$$I_x^- = - g_m.V_z \quad (5)$$

These equations show the all possible implementation of CDTA. Here the voltage of the terminal p, n, z and x are shown as V_p , V_n , V_z and V_x. For CDTA +- the following equations are true.

$$\begin{bmatrix} I_z \\ I_{x+} \\ I_{x-} \\ V_p \\ V_n \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & -1 \\ g & 0 & 0 & 0 & 0 \\ -g & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} V_z \\ V_{x+} \\ V_{x-} \\ I_p \\ I_n \end{bmatrix}$$

III. PROPOSED CIRCUIT

Inverse high pass filter is a filter that passes the frequency higher than the cut off frequency and attenuate the frequency lower than the cut off frequency. The inverse low pass filter is a filter having inverse transfer characteristics of the high pass filter. It means it passes the frequency lower than the cut off frequency and attenuates the frequency higher than the cut off frequency.

Standard equation of Inverse High Pass Filter.

$$H_{IHPF}(S) = 1 + \frac{W_o}{Q_o S} + \frac{W_o^2}{S^2} \qquad (6)$$

The proposed Inverse High Pass Filter is shown in fig 2, Transfer function of this filter is shown below.

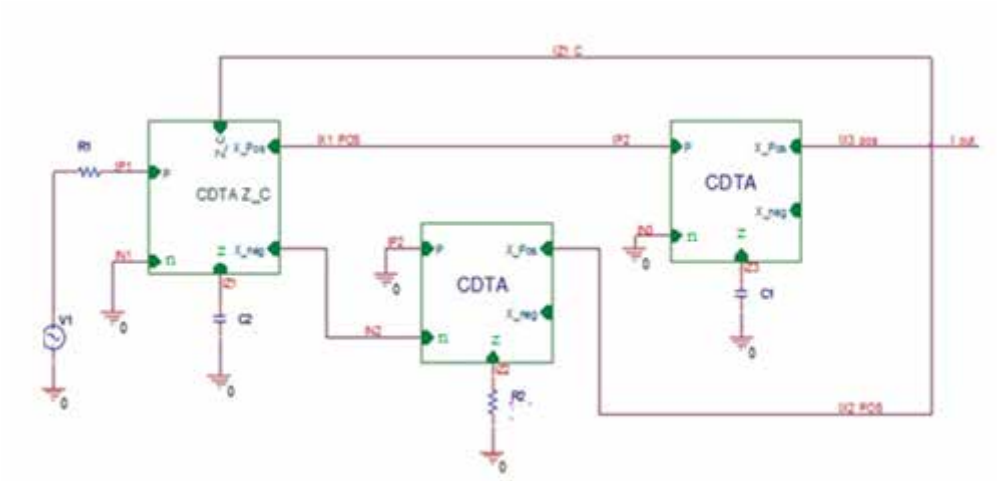


Fig. 2. Schematic Diagram of Proposed Inverse High Pass Filter

$$I_{p1} = \frac{V_{in} - V_{p1}}{R}$$

$$I_{p1} = \frac{V_{in} - 0}{R}$$

$$I_{p1} = \frac{V_{in}}{R} \qquad (7)$$

Now By Using CDTA Property

$$I_{z1} = I_{p1} - I_{n1}$$

$$I_{z1} = I_{p1} - 0$$

By using equation

(7)

$$I_{z1} = \frac{V_{in}}{R_1} \tag{8}$$

$$I_{x1}^{+} = g_{m.} V_{z1}$$

$$I_{x1}^{+} = g_m . \frac{V_{in}}{R_1 S C_1}$$

$$I_{x1}^{+} = \frac{g_m . V_{in}}{R_1 S C_1} \tag{9}$$

$$I_{z2} = I_{p2} - I_{n2}$$

$$I_{z2} = 0 - I_{n2}$$

$$I_{z2} = - I_{n2}$$

$$I_{n2} = I_{x1}^{-}$$

According to CDTA property output are equal in magnitude but opposite in phase.

By using equation (9)

$$I_{n2} = - \frac{g_m V_{in}}{S R_1 C_1}$$

$$I_{z2} = \frac{g_m . V_{in}}{S R_1 C_1} \tag{10}$$

$$I_{x3}^{+} = g_m V_{z3}$$

$$I_{x3}^{+} = g_m . I_{z3} . \frac{1}{S C_2}$$

$$I_{z3} = I_{p3} - I_{n3}$$

$$I_{z3} = I_{p3} - 0$$

$$I_{p3} = I_{x1}^{+}$$

By using equation (9)

$$I_{z3} = \frac{g_m V_{in}}{R_1 S C_1} \tag{11}$$

$$I_{x3}^{+} = g_m g_m \frac{V_{in}}{S R_1 C_1} . \frac{1}{S C_2}$$

$$I_{x3}^{+} = g_m^2 \frac{V_{in}}{S^2 R C_1 C_2} \tag{12}$$

$$I_{x2}^{+} = g_m . V_{z2}$$

$$I_{x2}^{+} = g_m I_{z2} R_2$$

By using equation (10)

$$I_{x2}^{+} = g_{m.} g_m \frac{V_{in}}{S R_1 C_1} . R_2$$

$$I_{x2}^{+} = g_m^2 . \frac{V_{in} . R_2}{S R_1 C_1} \tag{13}$$

Now Final Output is

$$I_{out} = I_{z1} + I_{x2}^{+} + I_{x3}^{+}$$

By using equation (8), (13) and (12)

$$I_{out} = \frac{V_{in}}{R_1} + \frac{g_m^2 V_{in} R_2}{S R_1 C_1} + \frac{g_m^2 V_{in}}{S^2 R_1 C_1 C_2}$$

$$\frac{I_{out}}{V_{in}} = \frac{1}{R} + \frac{g_m^2 R_2}{S R_1 C_1} + \frac{g_m^2}{S^2 R_1 C_1 C_2} \tag{14}$$

By comparing equation (12) with standard Inverse High Pass Filter equation (6)

$\omega_o^2 = g_m^2 / R R_2 C_1 C_2$

$\omega_o = g_m / \sqrt{R R_2 C_1 C_2}$

$2\Pi f_o = g_m / \sqrt{R R_2 C_1 C_2}$

$f_o = g_m / 2\Pi \sqrt{R R_2 C_1 C_2}$

and

$$\frac{\omega_0}{Q} = g_m^2 / RC_1$$

Therefore

$$Q = \sqrt{\frac{RC_1}{g_m R_2 C_2}}$$

Phase angle of Inverse High Pass Filter

$$\Phi f = \Phi H_{IHPF}(jw) = \frac{g_m^2 R_2}{jwRC_1} + \frac{g_m^2}{(jw)^2 RC_1C_2} + \frac{1}{R}$$

$$\Phi f = \frac{-jg_m^2 R_2}{wR_1C_1} - \frac{g_m^2}{w^2 R_1C_1C_2} + \frac{1}{R_1}$$

$$\Phi f = \frac{1}{R_1}\left(\frac{jg_m^2 R_2}{wC_1} - \frac{g_m^2}{w^2 C_1C_2} + 1\right) \quad (15)$$

By using equation (15)

$$\Phi f = \tan^{-1}\left(\frac{g_m^2 R_2 / wC_1}{1 - g_m^2 / w^2 C_1C_2}\right) \quad (16)$$

IV. SIMULATION RESULTS

To verify the proposed inverse filter response of the ILPF, IHPF and IBPF are simulated on PSPICE using 350 nm Level 3 CMOS Process Parameter provided by MOSIS (Agilent).A ±3.5 V Supply voltage is chosen. Magnitude and phase response of the system is obtained by connecting capacitance and resistance to the filter. The CDTA is used as the basic building block for all inverse filters.

Proposed inverse high pass filter shown in Fig. 2 is simulated by selecting R1=1KΩ, R2=10KΩ, C1=C2=10nF, a 100mV AC source is applied to the inverse high pass filter. Fig. 4 shows the AC Response (Frequency) for the applied input.

Fig. 5 shows the phase response for the IHPF for the above values of resistance and capacitances.

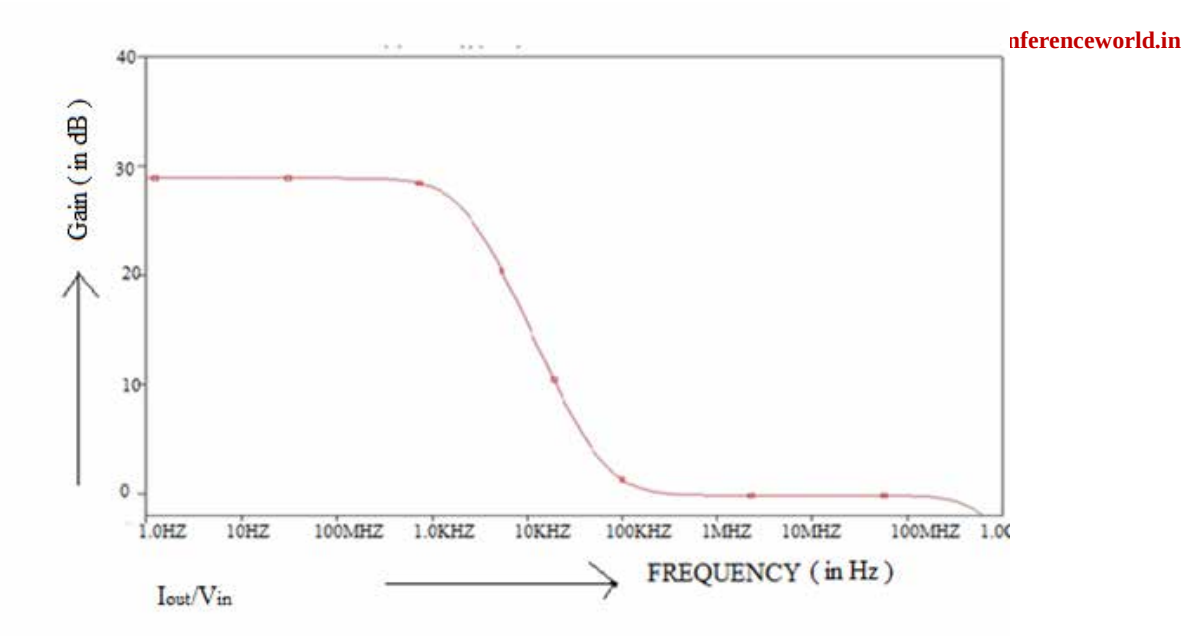


Fig. 4 Magnitude response of Inverse High Pass Filter

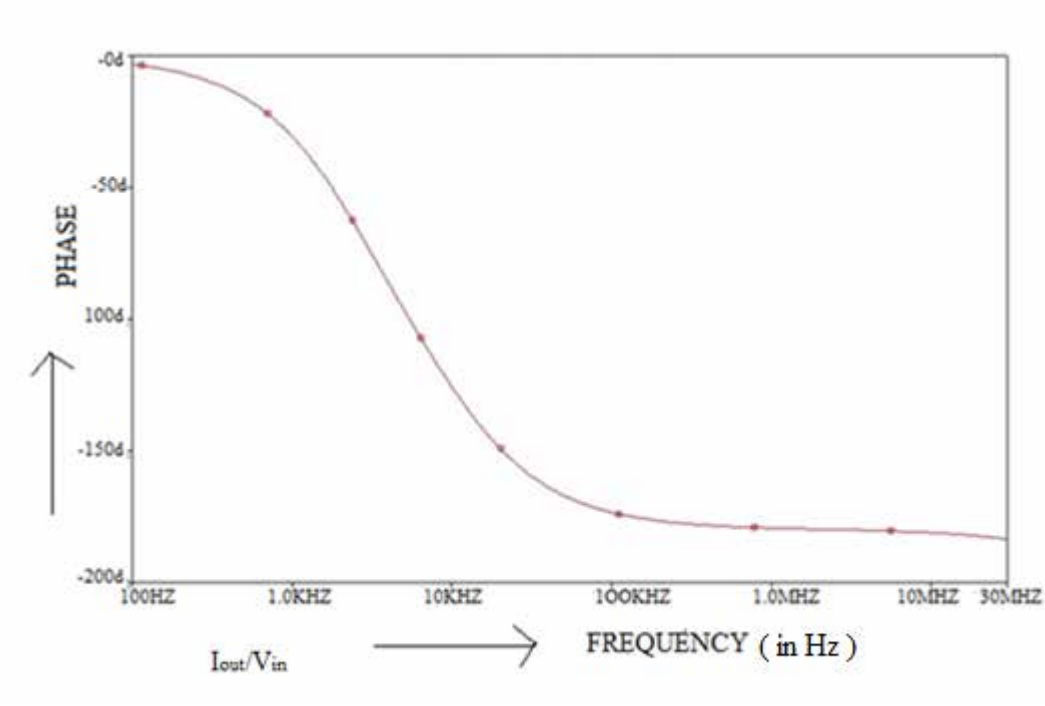


Fig. 5 Phase response of Inverse High Pass Filter

V. CONCLUSION

This dissertation is focused on analysis and performance of Inverse High Pass Filter (IHPF) using Current Differentiating Transconductance Amplifier (CDTA) with desirable frequency response. The basic building block performance analysis of the filter is done by frequency analysis on P- SPICE. Simulation result of these filters is very close to theoretical value.

REFERENCES

[1] A. Watanabe, "Formant estimation method using inverse-filter control," IEEE Transactions on Speech and Audio Processing, vol. 9, no. 4, pp. 317–326, 2001.

[2] O. Kirkeby and P. A. Nelson, "Digital filter design for inversion problems in sound reproduction," Journal of theAudio Engineering Society, vol. 47, no. 7-8, pp. 583–595, 1999.

[3] Z. Zhang, D. Wang, W. Wang, H. Du, and J. Zu, "A group of inverse filters based on stabilized solutions of fredholmintegral equations of the first kind," in Proceedings of the IEEE International Instrumentation and Measurement Technology Conference, pp. 668–671, May 2008.

[4] Neeta Pandey and Rajeshwari Pandey , " Current Mode Full Wave Rectifier Based on a Single MZC-CDTA", ISRN Electronics, vol. 2013, article id 967057, Hindawi Publication Corporation, 2013.

[5] A. Leuciuc, "Using nullors for realisation of inverse transfer functions and characteristics," Electronics Letters, vol. 33, no. 11, pp. 949–951, 1997.

[6] B. Chipipop and W. Surakampontorn, "Realization of current mode FTFN-based inverse filter," Electronics Letters, vol. 35, no. 9, pp. 690–692, 1999.

[7] N. A. Shah, Munajah Quadri and S. Z. Iqbal, "CDTA based Transimpedence Type First Order All Pass Filter." Indian Journal of Pure and Applied Physics, vol. 44, no. 3, pp. 269–271, June 2008

[8] M. Tanter, J. F. Aubry, J. Gerber J. L. Thomas and M. Flink, "Optimal Focusing by Spatio Temporal Inverse Filter", International Journal, vol. 8, no. 9, pp. 137-705, 2001.

[9] N. A. Shah, M. Quadri, and S.Z. Iqbal, "High output impedance current-mode all pass inverse filter using CDTA," Indian Journal of Pure and Applied Physics, vol. 46, no. 12, pp. 893–896, 2008.

[10] H. Y. Wang and C. T. Lee, "Using nullors for realisation of current-mode FTFN-based inverse filters," Electronics Letters, vol. 35, no. 22, pp. 1889–1890, 1999.

[11] Rajeshwari Pandey, Neeta Pandey, Tushar Negi and Vivek Garg, "CDBA Based Universal Inverse Filter", ISRN Electronics, vol. 2013, article id 181869, Hindawi Publication House, 3 February 2013.

[12] D. Biolek, "CDTA-building block for current-mode analog signal processing," in Proceedings of the ECCTD'03, vol. 3, pp. 397–400, Krakow, Poland, 2003.

[13] Biolek D, Biolkova V., "Universal biquads using CDTA elements for cascade filter design", In: Proceeding of the CSCC, ISBN 960-8052-82-3(CD), Corfu, Greece, 2003.

REDUCING STORAGE REQUIREMENT WITH SECURITY ENHANCEMENT FOR BIOMETRIC UID SYSTEMS

[1]Anjana.P, [2]Betty.P

[1]PG Scholar, [2]Assistant Professor, Department of CSE,

Kumaraguru College of Technology, Coimbatore (India)

ABSTRACT

Biometric UID system is a technique that is used to identify a person using quantifiable biological or behavioral characteristics along with demographic information. Biometric UID system had been used in vast area of applications providing identification and security in major aspects .UID system contains unique identification number that can establish a person identity at any place, any time. Biometric UID system provides a comprehensive view of its vast inventory of assets. Though Biometric process has several advantages it is vulnerable to attacks which compromise the security objectives of the system .Confidentiality ,integrity , availability are the main properties of biometric security systems .In biometric UID systems storage , the template and database are the crucial parts .To overcome the security issues towards the template information, a cryptographic approach template security is proposed which will use a non –invertible transform approach with key binding which eventually reduces the storage requirements. The proposed system of biometric template protection will be worth challenging the existing biometric template protection methods used in the biometric UID systems.

Keywords: Biometric Template-Security- Encryption Methodology –Irrevocability- Projection – Transformation-Cube

I INTRODUCTION

Identification is very much important because of finding the person under mass surveillance [1]. Authentication is also needed in various sectors as internet evolves everywhere. Today all technology evolves with the touch of internet and almost everything we do online which requires online authentication, identification and e-transaction. As internet grows consequently identification and authentication are also needed. To identity the people under surveillance identification is much needed [1]. Traditional approach of identification and authentication involves user name and password. Password based system is such a messy as people always prefers easy password and uses the same password for many accounts is makes the job of hackers very easy. Thus unlike an password system , biometrics which is an bodily element and uses the biometric traits as password .Biometric traits is an bodily element so users doesn't want to carry it anywhere nor to remember . Biometric traits provide the unique to a great certainty. Biometric system in which the biometric data used are very sensitivity and can't be false proof. Biometric database once compromised it is compromised forever.

A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample. Templates are used during the biometric authentication process .In biometrics, a fingerprint tem plate is the name used to describe a stored file in a fingerprint scanning system .When a fingerprint is entered in to the system, only a "template" of the fingerprint Is stored, not an image of the fingerprint .A fingerprint template is smaller than the actual fingerprint image and using the template instead of an image makes for faster processing time.

Biometric security has few characteristics which should be preserved to have a secure processing using these biometric features. These characteristics are very unique especially for the sensitiveness of biometrics. The characteristics are broadly classified into physiological and behavioral characteristics. Any distinguishing characteristics of an individual that can be measured and extracted from a biometric sample for the purpose of biometric identification. Biometric is mainly used to follow a simple rule of "Defend yourself against identity theft.

One of the most challenging characteristics of biometric is that these characteristics may be affected by changes in age, environment, disease, stress, occupational factors change in human interface [19]. These characteristic of biometric template can be handled using the approximate security algorithms in which storage issues are also concerned The user keys are replaced with biometric trait for flexible usage of the system.

Two most important concern of biometric system are security and storage of biometric templates. Storing such a template means that it requires more storage space and also it should be stored securely. These two concerns must be addressed in all biometric systems. If the biometric data is recorded in central database, privacy concerns may be higher. To satisfy the privacy concerns many encryption algorithms are used and for storage space reduction many cropping and size reduction algorithms are used.

Problems With large database make biometric identification process does not scale well with size and also search space will be high. Biometric templates are high dimensional and has no linear ordering or sorting exists for biometric data. Biometric templates with no privacy means other person to easily theft the person's individuality and it will severe issue since biometrics once compromised it is compromised forever.

Biometric traits follow very important characteristics irrevocability. Thus to maintain its characteristics biometric must be reversed .Unlike password system in which once password are compromised we can demand for another password .But in biometric system in which once the biometric traits are compromised then we can't change or demand for another biometric as it is bodily element of an individual .Thus biometric can't be replaced . Thus securing these biometric traits are growing now and many technology and methodology have been followed in various identification system.One of the mandates given to UID is to define usages and applicability of authentication for delivery of various services. UID provides authentication using the user's demographic and biometric information. The biometric traits are secured in database, communication channel, etc.

Various techniques have been discussed along with advantages and disadvantages in the following sections with the explanation of the algorithm being discussed.

II REVIEW ON VARIOUS BIOMETRIC TEMPLATE PROTECTION TECHNIQUES

Biometric has been used in various applications for its uniqueness and authentication [1] .While using biometric systems, only the feature which are extracted from the biometric are used. These feature of the biometric trait are called as biometric template and these template are stored in the database and used during enrollment and

verification process .During the process the biometric traits are taken as input using the sensors and they are converted into digital information and these digital information of a biometric traits are called as template and used for the authentication purpose. These biometric template has to be protected because biometric once compromised then it is compromised forever. Thus to maintain its irrevocability characteristics template protection is needed. Thus if a user A wants to create a mail account with another user B using his biometric , the user A may think that B is an imposter and he is interested in his account or the communication channel is vulnerable similarly the user B may be imposter and later deny his service and also communication channel is vulnerable. Thus to avoid these vulnerabilities template protection is needed. Compromising the biometric traits makes an individual to lose his identity and it cannot be replaced. The biometric template can be protected using various methodologies.

Double encryption method [4] It is two ways secured biometric authentication system. .It is safeguard using two different encryption algorithm in both client and server side .It involves two level security so it provide better security than any other security methodology In client side it uses RSA algorithm and Server side it uses 3 DES algorithm . Advantages of this technology involve high accuracy and it addresses all features of biometrics. Disadvantages of this technology involves long procedure of algorithm .Thus using the two way encryption enhances provable protection against all the attacks like replay, tracking and compromising key of the user .Future work of this technology is that it can be applied to other biometric recognition system and any cryptographic algorithm. This technology will be efficient in securing the template in communication channel .Thus it server dependency for the key generation sometimes will be disadvantages. In this chaos phenomenon which over takes encryption methodology are discussed.

Multilevel encryption method [3]This method is used for template protection using double encryption method .It involves two levels of encryption using fuzzy vault and DAES algorithm This particular biometric verification system uses multibiometric features and fuzzy vault scheme which is encoded using DAES algorithm. As fuzzy vault issued it provides an additional layer of security. It involves in extracting the feature from an biometric image and the vector are transformed .The transformed vector are protected using fuzzy vault .The symmetric keys are used as the second level of security which encode the vault used in the first level. Advantages of using this approach is that it uses multiple impression of iris which in turn provides high accuracy and It reduces multiple impression of same iris .This particular methodology deals with securing the template in database .This methodology doesn't depends on the server for the key generation and it reduces the dependency of the server than the previous double encryption methodology.

Hybrid encryption method[2] This methodology uses hybrid encryption methodology .It uses symmetric key algorithm and RSA Asymmetric key algorithm. It is know that hybrid system increases reliability of verification, capture unique and it is difficult to spoof. Thus this methodology provides effective and efficient mechanics for confidentiality and authentication and provides combination of biometric attributes. By following such a hybrid methodology it provides higher performance which is more interactive and provides high quality .Performance and key generation time are decreased. The methodology of using such an algorithm is known well.

Encryption method	Algorithm used	Discussion
Double encryption	RSA and 3DES algorithm	On client and server side
Multi level encryption	Fuzzy vault and DAES algorithm	On template database
Hybrid encryption	Symmetric and RSA algorithm	On template database

Table 1: Comparative study of key generation methodology

In [5] a robust security model for biometric template protection using chaos phenomenon is considered. This phenomenon uses a feature transform approach and it generates a transformation function which is applied to the biometric template and only the transformed template is stored in the database. Unlike key binding approach the keys are generated directly from the biometric feature. Choas variables are usually generated by logistic map .Logistic map is a one-dimensional quadratic map .Logistic map are used to generate the chaotic evolutions and the chaotic system are deterministic and sensitive to the initial values. It has a complex active action which can be used to protect data content. The session keys are used to protect the encrypted biometric template .These session keys are generated using chaos phenomenon. This session keys are randomly generated to ensure the security of a communication sessions

Reinhard et al. [10] presents Two-Factor Biometric Recognition with Integrated Tamper-protection Watermarking. It uses the application of semi –fragile watermarking and uses a two way authentication schemes using iris recognition and smart cards. One of the ideas is to combine biometric technologies and watermarking is "biometric watermarking" [18]. The aim of watermarking is to employ biometric templates as "message" to be embedded in classical robust watermarking applications like copyright protection in order to enable biometric recognition after the extraction of the watermark (WM). Semi-fragile WM is used to embed the template data stored on the smart-card into the sample data acquired at the authentication site. In this approach included the experimental results in the case of an iris recognition system, that indeed semi-fragile integrity verification is achieved [10].

In [11] uses a two watermarking algorithms .It uses discrete wavelet transforms and LSB based watermarking algorithm. It embeds a face template in a finger print image. In this technique they have used fingerprint as a cover image and facial feature as watermarking. The features from the face are extracted using the 2D Gabor filter. It works by watermarking embedded algorithm and extraction algorithm.

III. PROPOSED APPROACH

Biometric template protection is done using key generation methodology in proposed approach. Key generationmethodology is a method of generating the key using some technical approach like hashing or salting .It is different from key binding approach in which key are generated using cryptographic approach and binding the keys with biometric template. In this approach the keys are generated directly from the biometric feature without using cryptographic approach. Random projection are used to protect a sensitive data like biometric.

In this designed biometric hashing technique [5] uses session key which are generated by using the chaos phenomenon.This method is focus on the attack on the template database like smart card, central repository and sensing devices. To protect the database from the imposter it uses the transformation to secure the biometric template .In chaos phenomena it uses the stored encryption biometric template for the session key which are randomly generated .It comes under hashing and salting approach .The advantages of using this methodology is that, session key cannot be duplicated and also guessing of session key is difficult .It is robust method.

It uses preliminary [5] non-invertible transform approach which are based on random projection. This chaotic behavior of logistic map to build projection matrix based on biometric template and identity .It is non-invertible transformation with no need of user's key .Logistic map are used to construct multiple random vectors and these vectors are stored in spiral cube .And these methodology meets all the requirement of revocability, diversity and security.

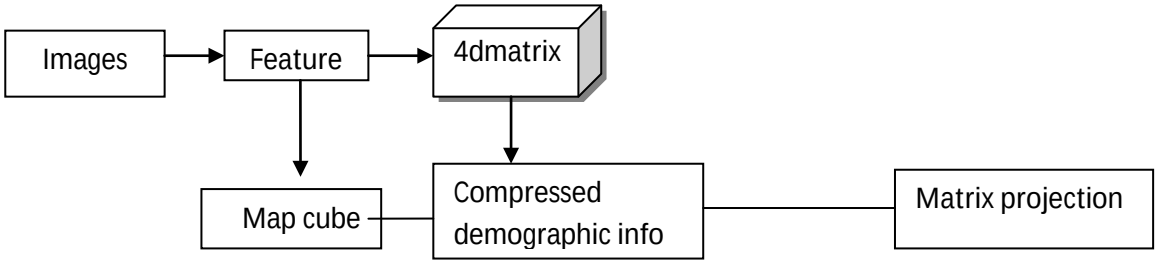


Fig1: Proposed Architecture

We construct the projection matrices for each identity using the 4d matrixand the *map cube.* Assuming that we calculate the projection matrix of identity 1 (first vector of the map cube), the first value of the quantified vector (size) of this identity corresponds to the first cell in the spiral cube, and so on for the other values.

The 4d matrixes are constructed using the 4 dimensional projection of feature vector generated form the biometric trait. The feature vector follows mathematical concept along with gradient value of each feature vector .Once the 4d matrix are constructed .Another matrix of feature vector which is extracted from different region of interest from same biometric trait which is map cube .These two cubes are transformed and transformed matrix are used in the identification system.

The existing technique meets the requirements of revocability, diversity and security [5]. Knowing that multiple acquisitions of the same biometric trait do not yield an identical set of features, the dynamics of our approach allow us to create different templates for the same identity in the presence of these variations. In addition, we can protect a compromised template by changing partially the map cube. We change, specifically, the quantized vector corresponding to the identity of the compromised template, either by redoing the quantization or by changing partially this quantized vector.

To improve a security of biometric template used in the UID system and to minimize the duplication of identity and to reduce the storage requirement used initially separate algorithm for compression and security of biometric traits are used depends on the application it has been deployed. Key binding and invertible transformation for biometric template storage isproposed. As it is the key binding technology it generates the key using the biometric traits .The feature vector from the biometric are obtained which are used as the key such that it is independent of user's key. Once the key are generated it uses the mathematical concepts of projection by mapping the template with the orthogonal matrix. The projection results in the generation of transformed function. The key generation

for the orthogonal matrix is not from the user key, it is also generated from the feature vector of the biometric traits used.

Proposed technique address the weak point of existing method of redoing the training task when order of cells are changed in 4d matrix .Proposed approach uses the concept of projection methodology with few challenges in application of the strategy .Thus the 4d matrix are constructed using logistic map and map cube unlike the quantized vector, the projection approach are altered to address better security and storage concerns.

Session keys are generated using transformation approach. Both cubes are formed using feature vector which is extracted from the biometric trait. Thus the keys are generated without any approach like key binding.4d matrix cube are constructed using logistic map .Map cube are generated using the feature vector of different region of interest as it is known that region of interest are not uniform. Feature vector are generated from the biometric trait and feature vector are used to construct the spiral cube and map cube. Projection of these cube are used to secure the biometric template.

In the proposed approach uses the unimodal biometric trait iris. Iris is the unique feature of all biometric. It provides highest unique characteristics. For feature vector generation established a boundary of iris and defines zones for analysis within the co-ordination system. As analytic behavior of iris cannot be defined, features are isolated using houghtransforms. Compressed demographic information is mapped with the projected matrix in the database for unique identification in UID system.

It has been estimated that the processing time is comparatively less than the existing approach. Once the spiral cells order are changed it is not necessary to redo the training templates .This is because map cube are not quantified and stored .Map cube are just an another feature vector from the biometric trait. These two cubes are projected and stored as transformed matrix. The biometric feature vector are not stored in extracted form .The vector are transformed and stored in transformed format. The proposed approach is experimented using the uni-modal biometric traits iris .

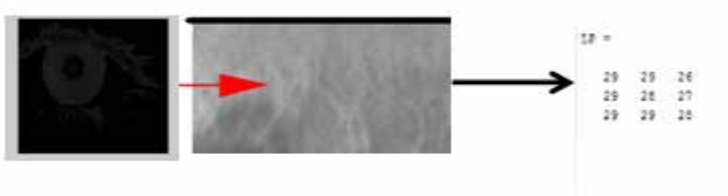
IV MODULE DESCRIPTION

1. Feature Extraction

Feature is extracted from biometric trait instead of processing all unwanted region of interest.

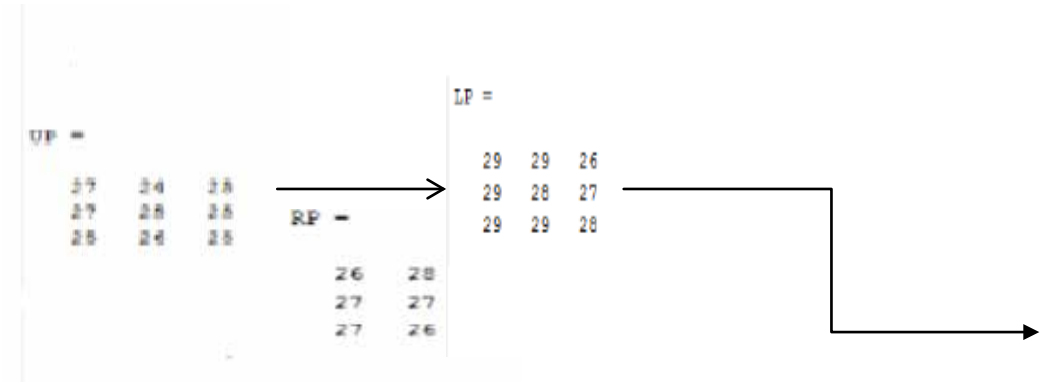
2. Feature vector generation

Most biometric technique do not operate on raw material, they generally operate on the feature vector



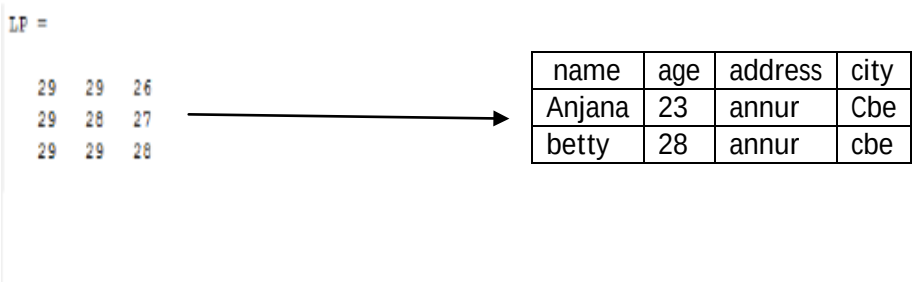
3. Matrix projection

The feature vector are projected and stored as matrix form which is the normalized form of biometric traits is obtained



4. Mapping of Demographic information

The demographic information are mapped with the protected matrix template of biometric system as it is UID system



name	age	address	city
Anjana	23	annur	Cbe
betty	28	annur	cbe

V. CONCLUSION

In this paper, proposeda new approach for biometric template protection .Logistic map vector is used to generate the vectors of projection. These vectors are stored in 4d matrix cube and map cube are formed from different region of interest, which in turn are used to generate the matrix of projection and depends on the templates to be protected.The security level of biometric system is improved to few extend using the new idea of key generating method. The security and storage parameters are both addressed in the paper. The mathematical concept helps to provide better security and storage space is minimized to few extend.

REFERENCES

[1] Collin soutar,Dannyroberge , Alex Stoianov ,Rene Gilroy , and B.V.K Vijaya Kumar, "Biometric encryption" BioscryptInc(formelymytec Technologies Inc.),5450 Explorer Drive ,Suite 500 Mississauga ,ONT L4W 5M1.

[2] ShwetaMalhotra, Chander Kant Verma, "A Hybrid Approach for Securing Biometric Template", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[3] Mohammed shahnawazNasir ,PrakashKuppuswamy , "implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm ",International Journal Of Innovative Research

In computer and communication enginnering (AN ISO:3297:2007 CERTIFIED ORGANIZATION) VOL 1,ISSUE 8, OCTOBER 2013.

[4] S.Kavinhariharasudhan,S.Ramamoorthy , " Double Encryption Based Secure Biometric Authentication System" ,ISSN:2231-5381 (2012).

[5] Maithili Arjunwadkar ,DR.R.V.Kulkarni , " Robust Security Model for Biometric Template Protection using Chaos Phenomenon" , computer applications (0975-8887) volume 3 –no 6 (2010)

[6] Moujahdi, Ghouzali, Mikram, Rziza,Bebis, "Spiral cube for Biometric Template protection", Springer-Verlag Berlin Heidelberg (2012)

[7] A. K. Jain and U. Uludag " Hiding fingerprint minutiae in images. In Proceedings of AutoID ", 3rd Workshop on Automatic Identification Advanced Technologies, pages 97–102, Tarrytown, New York, USA, March 2002.

[8] A. K. Jain, U. Uludag, and R. L. Hsu, " Hiding a face in a fingerprint image", In Proceedings of the International Conference on Pattern Recognition (ICPR'02), pages 756–759, Quebec City, Canada, August 2002.

[9] A.K. Jain and U. Uludag. Hiding biometric data. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(11):1494–1498, November 2003.

[10] Reinhard Huber1 , Herbert St¨ogner1 , and Andreas Uhl1,2 1 School of CEIT, "Two-Factor Biometric Recognition with Integrated Tamper-protection Watermarking ",Carinthia University of Applied Sciences, Austria 2 Department of Computer Sciences, University of Salzburg, 2007

[11] MayankVatsa ,RichaSingh,AfzeelNoore,MaxH.Hoack and Keith Morris, " Robust Biometric Image Watermarking for fingerprint And face template Protection", IEICE Electronics Express,vol 3,no-2 ,23-28,2006.

[12]MitaPaunwala&SupravaPatnaik, "Biometric Template Protection With Robust Semi – Blind Watermarking Using Image Intrinsic Local Property", International Journal of Biometrics and Bioinformatics (IJBB), Volume (5) : Issue (2) : 2011 28 ,2006

[13] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[14]. K. Bae, S. Noh, and J. Kim, "Iris feature extraction using independent component analysis," in Proceedings of the 4th International Conference on Audio- and VideoBased Biometric Person Authentication (AVBPA '03), vol. 2688, pp. 1059–1060,Guildford, UK, June 2003.

[15] J. Urias, D. Hidalgo, P. Melin, O. Castillo, "A New Method for Response Integration in Modular Neural Networks using Type-2 Fuzzy Logic for Biometric Systems", IJCNN 2007, International Joint Conference on Neural Networks, pp. 311 – 315, 2007.

[16]. Zadeh, L.A.: Fuzzy sets. Information and Control 8 (1965)

[17] Sachenko, ArkadiuszBanasik, and Adrian Kapczyński , "The Concept of Application of Fuzzy Logic in Biometric Authentication Systems Anatoly "Silesian University of Technology, Department of Computer Science and Econometrics, F. D. Roosevelt 26-28, 41-800 Zabrze.

[18] Mukhwinder Singh* Tripatjot Singh Panag "Heterogeneous Multimodal Biometric System with Fuzzy Vault Template Security" , International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Volume 4, Issue 7, July 2014 ISSN: 2277 128X

[19] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proc. of the IEEE, vol. 92, no. 6, pp. 948–960, 2004.

[20] Christian Rathgeb and Andreas Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics" , 2007

[21]Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometrickey generation with biometric helper",in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications,pp.2145-2150, Singapore, June 2008.

[22] N. K. Ratha, J. H. Connell, R. M. Bolle,"Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, 40(3), pp. 614-634, 2001.

[23] R. M. Bolle, S. Pankanti, N. K. Ratha,"Evaluation techniques for biometrics based authentication systems (FRR)", Proceedings 15th International Conference on Pattern Recognition, vol.2, pp. 831 -837, 2000.

[24]Ari Juels, Madhu Sudan, "A Fuzzy Vault Scheme", IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.

[25] MohamadAbdolahi, MajidMohamadi, Mehdi Jafari, "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[26]P.U. Lahane, Prof. S.R. Ganorkar, "Efficient Iris and Fingerprint Fusion for Person Identification", International Journal of Computer Applications (0975 – 8887), Volume 50– No.17, July 2012.

[27] C.Hesher, A.Srivastava, G.Erlebacher, "A novel technique for face recognition using range images" in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2007.

[28] T. A. M. Kevenaar, G. J. Schrijen, M. vanderVeen, A. H. M. Akkermans,and F. Zuo, "Face recognition with renewable and privacy preservingbinary templates," in Proc. AutoID, 2005, pp. 21–26.

[29] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9,pp. 1081–1088, September 2006.

[30] T. A. M. Kevenaar, G. J. Schrijen, M. vanderVeen, A. H. M. Akkermans,and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. AutoID, 2005, pp. 21–26.

INITIATED DISCHARGE DUE TO ROCKET ASCENSION (IN.D.R.A)

Shantanu Bihani[1], Sumit Dhangar[2], Ajinkya Korane[3]

[1]UG Student, Dept of Computer Engineering, [2,3]UG Student, Dept of Mechanical Engineering,
Sandip Foundation's- Sandip Institute of Technology and Research Centre, Nashik, India

ABSTRACT

Globalisation, Industrialization, increase in population and increase in the machine dependence has led to a tremendous increase in the power demand but the comparative generation of power is not up to the mark. Hydro power plants need lot of water flow, nuclear and thermal power plants need non renewable energy forms in tremendous amount as well as there are many safety precautions to be taken. Earth resources needed for power generation are depleting but the demand of power is increasing! Its the cry of the hour to find out either an alternative power source or an alternative resource for power generation. Trapping and harnessing of natural electricity i.e. lightning with the help of rocketry and basic electrical concepts of conductors and capacitors this alternative of power generation resources as well as an alternative of power can be generated. This power generation includes study of chemical properties of substances, stress and strain i.e. the bearing capacity of metals, combustion properties of the fuels (chemicals) and electrical properties of conductors and capacitors. It includes calculation work for a proper functioning as well as designing of the research project.

***Keywords*: Globalization, Non Renewable Resource, Depletion, Alternative Power Supply, Lightning, Natural Electricity, Trapping and Using.**

I. INTRODUCTION

A rocket is a missile, spacecraft, aircraft or other vehicle that obtains thrust from a rocket engine. Rocket engine exhaust is formed entirely from propellants carried within the rocket before use. Rocket engines work by action and reaction. Rocket engines push rockets forward by expelling their exhaust in the opposite direction at high speed. Rockets rely on momentum, air foils, auxiliary reaction engines, gimbaled thrust, momentum wheels, deflection of the exhaust steam, propellant flow, spin, and/or gravity to help control flight.

Rockets are relatively lightweight and powerful, capable of generating large accelerations and of attaining extremely high speeds with reasonable efficiency. Rockets are not reliant on the atmosphere and work very well in space. Chemical rockets are the most common type of high power rocket, typically creating a high speed exhaust by the combustion of fuel with an oxidizer. The stored propellant can be a simple pressurized gas or a single liquid that disassociates in the presence of a catalyst (mono propellants), two liquids that spontaneously

react on contact (hypergolic propellants), two liquids that must be ignited to react, a solid combination of one or more fuels with one or more oxidisers (solid fuel).

II HISTORY

Rockets for military and recreational uses date back to at least 13th century China. Significant scientific, interplanetary and industrial use did not occur until the 20th century, when rocketry was the enabling technology for the Space Age, including setting foot on the moon. Rockets are now used for fireworks, weaponry, ejection seats, launch vehicles for artificial satellites, human space flight, and space exploration.

1232: A common claim is that the first recorded use of a rocket in battle was by the Chinese in 1232 against the Mongol hordes at Kai Feng Fu.

1792: In 1792, the first iron-cased rockets were successfully developed and used by Hyder Ali and his son Tipu Sultan, rulers of the Kingdom of Mysore in India against the larger British East India Company forces during the Anglo-Mysore Wars.

1926: On 16 March 1926 Robert Goddard launched the world's first liquid-fueled rocket in Auburn, Massachusetts.

1943: In 1943, production of the V-2 rocket began in Germany. It had an operational range of 300 km (190 mi) and carried a 1,000 kg (2,200 lb) warhead, with an amatol explosive charge.

Current Day: Rockets remain a popular military weapon. The use of large battlefield rockets of the V-2 type has given way to guided missiles. However rockets are often used by helicopters and light aircraft for ground attack, being more powerful than machine guns. Shoulder-launched rocket weapons are widespread in the anti-tank role due to their simplicity, low cost, light weight, accuracy and high level of damage.

III PROJECT WORK

The project aims at the generation of electricity by harnessing and trapping of the natural electricity i.e. lightning!

The project works on the principles of rocketry and aeronautics. Properties of conducting materials is at a great use here in this project.

3.1 Principle of Working

Aerodynamic bodies and aeronautics basic principles along with conducting capacity, heat bearing capacity, energy storing capacity of conductors and capacitors are used. The basic principles and laws of general physics and Electrical engineering are used.

3.1.1 Rocketry

The rocket motor we use in this project is a rocket motor which has a solid combination of one or more fuels with one or more oxidisers i.e. a solid fuel rocket motor.

1)Types of Solid Fuel Rocket Motors:

A) B-200 (“H”- Class)
B) C-400 (“I”- Class)
C) A-100 (“G”- Class)

D) A-100M ("G"- Class)

There are various other types of solid fuel rocket motors used but the widely used motors are the ones given above. The class of the rocket is determined according to the fuel used, thrust produced, and the distance covered by the rocket. The solid fuel rocket motors consist of various types of propellants [1].

3.2 Types of Propellants

a) Potassium Nitrate/ Sucrose Propellant (KNSU)

b) Potassium Nitrate/ Dextrose Propellant (KNDX)

c) Potassium Nitrate/ Sorbitol Propellant (KNSB)

Our project work includes the use of C-400 motor and KNSU propellant.

3.2.1 C-400 Solid Fuel Rocket Motor:

The C-400 rocket motor was developed in 1973 (originally as the C-II motor), a few months after the B-200 motor was developed. Its purpose was intended for boosting somewhat heavier rockets equipped with small payloads, as well as for proof testing of the parachute deployment method with higher altitude flights. It was expected that the rocket would achieve a peak height of about 2500-3000 feet (750-900 metres).

The thrust function for this motor is shown in Figure 1 below, achieving a maximum thrust of 325 pounds (1445 Newtons), and a total thrust time of 0.50 seconds. The total impulse is 106 lb-sec (470 N-s), which fits it into an " H " class designation. The high thrust combined with a short burn time provides for very quick acceleration of the rocket, which is beneficial for providing rapid aerodynamic stability of the rocket vehicle after departing the launch guide-rod. Having a free-standing grain, burning is completely unrestricted, meaning the hollow cylindrical grain burns on both inner and outer surfaces, as well as both ends. The performance graph was based on results from a static test of the motor (AST-13).

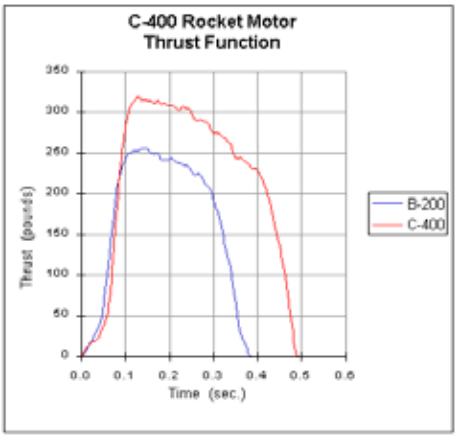


Fig. 1 C-400 Motor performance graph, with the B-200 motor performance shown for comparison

The performance of the motor is significantly influenced by the igniter. Non-pyrotechnic ignition would result in lower delivered impulse, lower maximum thrust, and an extended burn time (longer thrust build up duration). This motor is capable of boosting a 3 inch (7.6 cm) diameter rocket, with a mass of 5.5 lbs (2.5 kg), to an

altitude of over 3000 feet (900 metre) (this was typical of the rockets which I launched). If the rocket diameter is reduced to 2 inch (5 cm), the same rocket powered by the C-400 motor would achieve a peak altitude of close to 4000 feet (1.2 km) [1].

3.3 Designing of the C-400 Rocket motor

3.3.1 Nozzle

The C-400 nozzle is a conical profile, convergent-divergent, supersonic type. It has a 30 degree convergence angle, and a 12 degree divergence angle, and has an area expansion ratio of 16.8. It is machined from a single piece of cold-rolled (CR) steel bar stock, with polished inside flow surfaces. Of particular importance is the throat region, being the most critical with regard to motor performance. The nozzle contour is rounded at the throat to avoid sharp discontinuities in profile. The nozzle has a groove machined around the outer perimeter of the convergent section, to provide a recess for the nozzle retention screws. Six 1/4 inch hi-strength set screws, which engage into threaded holes in the casing, retain the nozzle. The nozzle is not normally removed once installed (propellant is loaded at the head end). To reduce leakage between the nozzle and casing, the casing is "rolled" around its circumference (after insertion of the nozzle) utilising a customised tool which effectively reduces the casing diameter locally, providing a nearly gas-tight seal. This tool is essentially the same as a constrictor *tool*, as used in HVAC applications. Filling the nozzle groove with silicone RTV will further reduce the likelihood of gas leakage.

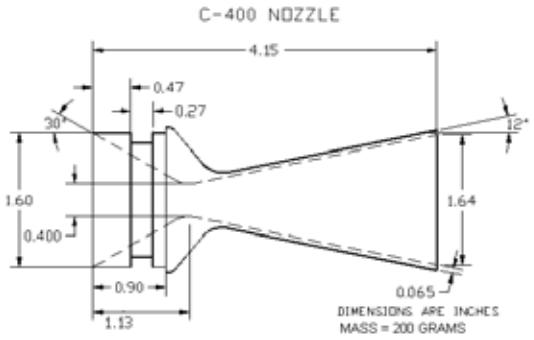


Fig. 2 Details of C-400 nozzle

3.3.2 Casing

The casing is made from seam welded steel tubing, specifically 1-1/2" Electrical Metallic Tubing (EMT).

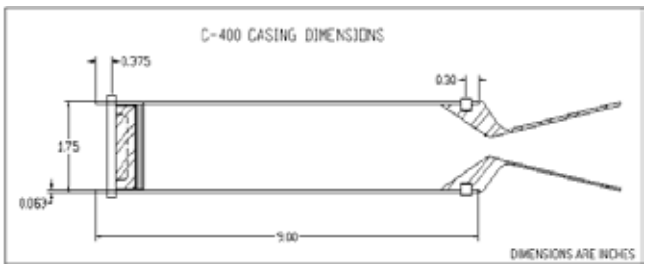


Fig. 3 C-400 Motor casing dimensions

3.3.3 Motor Head

The head is shown in detail in Figure 4.

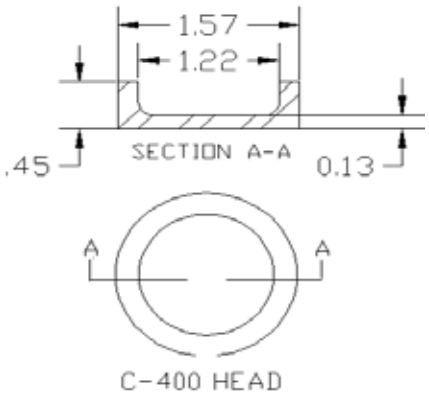


Fig. 4 Details of C-400 head **Fig. 5 Details of C-400 safety pin arrangement**

3.3.4 Propellant Grain

The C-400 motor is meant to be powered by KN-Sucrose propellant , cast as a hollow cylindrical free-standing grain, with unrestricted burning (i.e. all surfaces of the grain burn). The hollow core is normally 9/16 inch (1.43 cm) diameter. The maximum grain capacity is 380 grams. The grain is cast to size such that it is a slightly loose fit, and is loaded into the motor from the head end. Typical grain diameter is 1.58 inch (4.0 cm), and typical length of the cylindrical portion is 7 inch (17.8 cm). The steady-state burn profile is slightly regressive, with the (ideal) burning surface area initially 54 in^2 decaying to 47 in^2 prior to web burn through. This gives a Kn range of 430 (initial) and 370 (final).

Standard Composition (65/35 O/F): For the KN-sucrose propellant, with an oxidiser-fuel (O/F) ratio of 65/35, the theoretical combustion equation is as follows:

$C_{12}H_{22}O_{11} + 6.288\ KNO_3 \rightarrow 3.796\ CO_2 + 5.205\ CO + 7.794\ H_2O + 3.065\ H_2 + 3.143\ N_2 + 2.998\ K_2CO_3 + 0.274\ KOH$ at a pressure of 68 atmospheres, and where the following compounds are symbolised as:

TABLE I

Molecular Formulae for Components Of Propellant

sucrose	solid	$C_{12}H_{22}O_{11}$
potassium nitrate	solid	KNO_3
carbon dioxide	gas	CO_2
carbon monoxide	gas	CO
steam	gas	H_2O
hydrogen	gas	H_2
nitrogen	gas	N_2
potassium carbonate	liquid	K_2CO_3
potassium hydroxide	gas	KOH

3.5 Lightning

Lightning is a powerful sudden flow of electricity accompanied by thunder that occurs during an electric storm. The discharge will travel between the electrically charged regions within a thundercloud, or between a cloud and a cloud, or between a cloud and the surface of a planet. The charged regions within the atmosphere temporarily equalise themselves through a lightning flash, commonly referred to as a *strike* if it hits an object on the ground. There are three primary types of lightning; from a cloud to itself (intra-cloud or IC); from one cloud to another cloud (CC) and between a cloud and the ground (CG). Although lightning is always accompanied by the sound of thunder, distant lightning may be seen but may be too far away for the thunder to be heard. Many factors affect the frequency, distribution, strength and physical properties of a "typical" lightning flash in a particular region of the world. These factors include ground elevation, latitude, prevailing wind currents, relative humidity, proximity to warm and cold bodies of water, etc. To a certain degree, the ratio between IC, CC and CG lightning may also vary by season in middle latitudes. Lightning is usually produced by cumulonimbus clouds, which have bases that are typically 1–2 km (0.6-1.25 miles) above the ground and tops up to 15 km (9.3 mi) in height [2].

3.5.1 Establishing conditions necessary for lightning

In order for an electrostatic discharge to occur, two things are necessary: 1) a sufficiently high electric potential between two regions of space must exist; and 2) a high-resistance medium must obstruct the free, unimpeded equalisation of the opposite charges [2].

Fig. 6 Invoking and carrying of lightning using a conductor

3.5.2 Trapping Of Lightning

For trapping of light we need a conductor from the trapping point to the device where it is being trapped. So, here we use copper wire as a conductor. Copper being a very good conductor of electricity and as it is cheaply and abundantly available, he use of copper is most suitable for the project [3].

Fig. 7 Copper wires and Copper cables

The device used for trapping of any charge, current is known as a capacitor and the property to trap charge is known as capacitance [4].

1) Capacitance:

When a charge is delivered to a conductor its potential is raised in proportion to the quantity of charge given to it. At a particular potential a conductor can hold a given amount of charge. Capacitance *is the term to indicate the limited ability to hold charge by a conductor.*

Let charge given to a conductor be = q
Let V be the potential to which it is raised [5,6].

Then,

$q = CV$

C is constant for a conductor depending upon its shape size and surrounding medium. This constant is called capacitance of a conductor.

If V = 1 Volt than C = Q, thus capacitance is defined as the amount of electric charge in coulomb required to raise its potential by one volt.

If V = 1 Volt than C = Q, and Q = 1 Coulomb than C = 1 Farad thus one Farad is capacitance of a capacitor which stores a charge of one coulomb when a voltage of one volt is applied across its terminal.

2) Capacitor:

A capacitor or condenser is a device for storing large quantity of electric charge. Though the capacity of a conductor to hold charge at a particular potential is limited, it can be increased artificially. Thus any arrangement for increasing the capacity of a conductor artificially is called a capacitor. Capacitors are of many types depending upon its shape, like parallel plate, spherical and cylindrical capacitors etc. In capacitor there are two conductors with equal and opposite charge say +q and –q. Thus q is called charge of capacitor and the potential difference is called potential of capacitor.

3) Principle of capacitor:

Let A be the insulated conductor with a charge of +q units. In the absence of any other conductor near A charge on A is +q and its potential is V. The capacity of conductor A is therefore given by:

C = qV

If a second conductor B is kept closed to A than electrostatic induction takes place. –q units of charge are induced on nearer face of B and +q units of charge is induced on farther face of B. Since B is earthed the charge +q will be neutralised by the flow of electrons from the earth.

Potential of A due to self charge = V
Potential of A due to –q charge on B = -V'
Thus net potential of A = V + (-V') = V -V' which is less than V
Hence potential of A has been decreased keeping the charge on it fixed, hence capacitance has been increased. With the presence of B the amount of work done in bringing a unit positive charge from infinity to conductor A decreases as there will be force of repulsion due to A and attraction due to B. Thus resultant force of repulsion is reduced on unit positive charge and consequently the amount of work doe is less and finally due to this potential of A decreases. Therefore capacity of A to hold charge (Capacitance) is increased.

4) Dielectric Strength:

The material between the two conductors A and B as shown in figure above is always some dielectric material. Under normal operating conditions the dielectric materials have a very few free electrons. If the electric field strength between a pair of charged plates is gradually increases, some of the electrons may be detached from the dielectric resulting in a small current.

When the electric filed strength applied to a dielectric exceeds a critical value, the insulating properties of the dielectric material gets destroys and starts conducting between the two conductors A and B. This is called breakdown of dielectric which is fault condition for a capacitor bank. The minimum potential gradient required to cause such a break down is called the dielectric strength of the material. It measures the ability of a dielectric to withstand breakdown.

It is expressed as kV/mm. ss It is reduced by moisture, high temperature; aging etc. Below table gives dielectric strength of some.

TABLE II

DIELECTRIC STRENGHTH OF VARIOUS MATERIALS

Dielectric Material	Dielectric strength [kV/mm]
Air	3
Impregnated Paper	4 – 10
Paraffin Wax	8
Porcelain	9 – 20
Transformer Oil	13.5
Bakelite	20 – 25
Glass	50 – 120

Micanite	30
Mica	40 – 150

Dielectric Strength for capacitor is the maximum peak voltage that the capacitor is rated to withstand at room temperature. Test by applying the specified multiple of rated voltage for one minute through a current limiting resistance of 100 Ω per volt.

Fig. 8 A commercially used capacitor

Fig. 9 Block of commercial used capacitors

3.6 Calculations

- Electricity/ charge transferred during a single strike of lightning = 3 X 10^6 Volts.
- Resistance offered by the copper wire in the terms of specific resistivity = 1.78 X 10^{-8}
- Heat Loss during the transfer of charge = 10^5 J
- Therefore according to the Ohms law and by exempting the effect of heat, the power stored in the capacitor bank in just a single lightning is 3.3 X 10^6 W [7].

IV FUTURE SCOPE AND BENEFICIARIES

The power generated works as the best alternative to the power generated using non renewable resources. In the upcoming years the non renewable resources will get depleted and we will run short of power so such projects will serve the best at such times.

The project is beneficial for the under developed countries as well as developing countries. The production cost of the electricity using rockets is comparatively very less than the cost required for the production of hydro power as well as thermal and nuclear power. This type of power will be very useful for the villages and places in remote areas. This type of project is beneficial to every country using it.

V CONCLUSION

Thus upon further studies and development the need for the alternative and cheap power resource can be achieved. The proper use of conductors, study of the basic electrical properties of different materials, chemical composition and combustion properties of various chemicals and study of functioning of aerodynamic structures is done. Thus, the desired results are obtained.

VI ACKNOWLEDGMENT

Research on a specific topic as well as its project work takes a lot of efforts. The various components of the project require help from various people. In the making of the rocket components an intense amount of energy and guidance is required.

For this guidance and help we would like to thank many people. We would like to thank Mr. Ishwar Koli sir & entire workshop staff for helping us and guiding us in making of Rocket Nozzle and Rocket head and Prof. M. Khatik for allowing us to use college Chemistry lab for making of propellant. We would like to thank college authorities for believing in us and permitting us to do this project work. At last but not the least we would like to thank Prof. S. U. Gunjal for guiding us, helping us, also our friends Gunjan Chaudhari & Sumit Dhangar for always supporting us, in the entire project. The project wouldn't have been possible without their help.

REFERENCES

[1] http://www.nakka-rocketry.net/ accessed on 16th Sept' 2014

[2] http://en.wikipedia.org/wiki/Lightning accessed on 19th Sept' 2014

[3] S.Yoshida, C.J.Biagi, The initial stage process of wired triggered lightning as observed by VHF interferometry J.Geophys Res; vol 117, D09191,2012

[4] www.directindustry.com accessed on 19th Sept' 2014

[5] S.Yoshida, C.J.Biagi, Observations of stepping mechanism in a rocket and wire triggered lightning flash J.Geophys Res; vol 117, D09191,2012

[6] V. A. Rakov, Parameters of rocket triggered lightning, IJPEST, Volume-4 no. 1 March 2010, Pp. 80-85

[7] J. Schone, M. A. Uman, V. A. Rakov, Return Stroke peak current V/S Charge transfer in Rocket Triggered Lightning, J. Geophys, Res 117, D12107, doi: 101029 | 2009, JD013066, 2010

DESIGN AND IMPLEMENTATION OF LOGIC GATES USING FINFET TECHNOLOGY

G.Saranya[1], S.Jakkammal@Malarvizhi[2], K.Kalarani[3]

[1, 2] PG Scholar, [3.] Assistant Professor, Department of VLSI Design,

Theni Kammavar Sangam College of Technology, Tamilnadu, (India)

ABSTRACT

Scaling as one of the most important challenges from the technology viewpoint. The channel length of Field Effect Transistors (FETs) has passed from micrometers to tens of nano meters. However, drawbacks of scaling have the increase of short channel, parasitic, reliability and variability effects. To overcome the problems related to scaling, new transistor architectures have to be investigated. FinFET is the most promising double-gate transistor architecture to extend scaling over planar device. Multiple gates have better control over the SCEs. Particularly the FinFET technology provides superior scalability of the DG-MOSFETs compared to the planar MOSFET. Fin-FETs are predicted as one of the best possible candidates to replace the bulk MOSFETs. The FinFET technology power consumption compare with the CMOS technology. The two gates of a FinFET can either be shorted for higher performance or independently controlled for lower leakage or reduced transistor count. Analyzed different type of operation mode like Shorted Gate, Independent gate, and Low power mode.

Keywords: FinFET, Short Channel Effects (SCEs), Power Consumption, Logic gates, Different modes of operation

I. INTRODUCTION

The FinFET has been developed to overcome the problems faced by MOSFET. It is basically a multi gate Field Effect Transistor which has been scaled further of MOSFET. It has all properties similar to a transistor, but has some advantages on CMOS. As you can see the above figures, multiple drains and multiple sources, we can also use each pair of source and drain can be considered as a single transistor hence increasing the no of transistors in one FinFET.

MOSFET has some technical problems like i) short channel effects and ii) Corner Effect Corner .Effects has following problems: -

a) An enhancement of the leakage current at the edges of the active area adjacent to shallow trench isolation

b) Leakage enhancement is especially strong, if the gate electrode wraps around the corner of the active area

c) Corner effect leads to a not complete switching-off of the STI MOS transistors and worsens the transistor performance.

So to overcome the difficulty faced by traditional MOSFET, FinFET came into role and to make the transistors more efficient. Wider FinFET devices are built utilizing multiple parallel fins between the source and drain. Independent gating of the FinFET's double gates allows significant reduction in leakage current.

II MOSFET

Metal-Oxide-Semiconductor Field Effect Transistor is a three terminal device used for a variety of applications as per the requirement in different fields of electronics. It is used for amplifying or switching electronic signals. In MOSFETs, a voltage on the oxide-insulated gate electrode can induce a conducting channel between the two other contacts called source and drain. The channel can be of n-type or p-type and is accordingly called an nMOSFET or a pMOSFET (also commonly NMOS, PMOS).

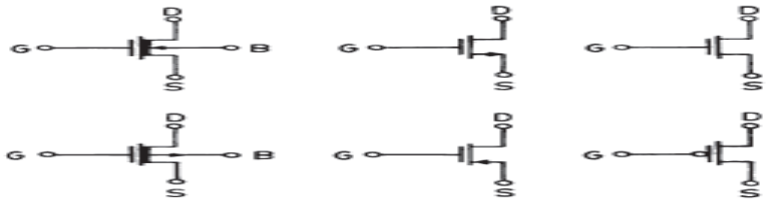


Fig.2.1 Symbols of NMOS & PMOS

G=GATE D= DRAIN S=SOURCE B = BULK

2.1 Operation of MOSFET

A traditional metal–oxide–semiconductor (MOS) structure is obtained by growing a layer of silicon dioxide (SiO_2) on top of a silicon substrate and depositing a layer of metal or polycrystalline silicon (the latter is commonly used). As the silicon dioxide is a dielectric material, its structure is equivalent to a planar capacitor, with one of the electrodes replaced by a semiconductor.

When a voltage is applied across a MOS structure, it modifies the distribution of charges in the semiconductor. If we consider a P-type semiconductor (with NA the density of acceptors, p the density of holes; p = NA in neutral bulk), a positive voltage, VGB, from gate to body creates a depletion layer by forcing the positively charged holes away from the gate insulator/ semiconductor interface, leaving exposed a carrier-free region of immobile, negatively charged acceptor ions. If VGB is high enough, a high concentration of negative charge carriers forms in an inversion layer located in a thin layer next to the interface between the semiconductor and the insulator.

Unlike the MOSFET, where the inversion layer electrons are supplied rapidly from the source/drain electrodes, in the MOS capacitor they are produced much more slowly by thermal generation through carrier generation and

recombination centers in the depletion region. Conventionally, the gate voltage at which the volume density of electrons in the inversion layer is the same as the volume density of holes in the body is called the threshold voltage. This structure with P-type body is the basis of the N-type MOSFET, which requires the addition of an N-type source and drain regions.

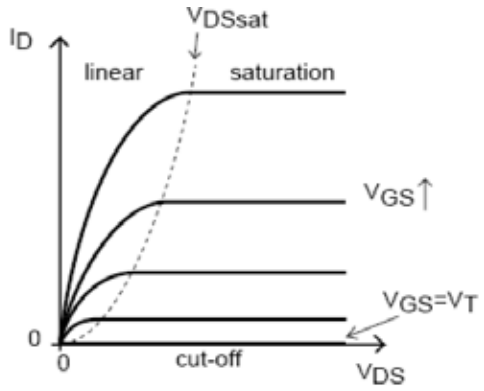


Fig.2.2: Operation of MOSFET

2.2 DG – MOSFET Structure

Currently standard CMOS technology can be replaced by DG MOSFETs technology to increase the integration capacity of silicon technology in the near future [5]. A DGSOI Structure consists, basically, of a silicon slab sandwiched between two oxide layers shows in Fig.2.3. The salient features of the DG MOSFETs are control of short-channel effects by device geometry, as compared to bulk FETs, where the short-channel effects are controlled by doping concentration; and a thin silicon channel leading to tight coupling of the gate potential with the channel potential. These features provide potential DG MOSFET advantages are reduced short channel effects which allows for a larger gate overdrive for the same power supply and the same off-current and better carrier transport as the channel doping is reduced.

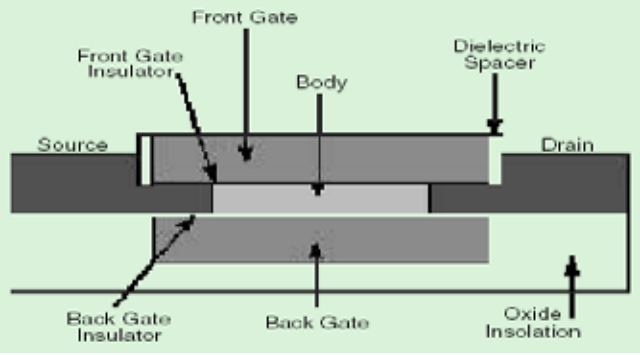


Fig.2.3: Cross Section of a Generic Planar DGFET

Basically there are 2 kinds of DG-FETs: (1) Symmetric: - In Symmetric DG-FETs have identical gate electrode materials for the front and back gates means gate electrode material is same for both gate. When symmetrically

driven, the channel is formed at both the surfaces. (2) Asymmetric: - In an asymmetric DG-FET, the top and bottom gate electrode materials can different. Channel is formed only in one surface.

There are three ways to fabricate the DG-FET

- Planar DGMOSFET
- Vertical DGMOSFET
- FinFET

Types 1 and 2 suffer most from fabrication problems, viz. it is hard to fabricate both gates of the same size and that too exactly aligned to each other. Also, it is hard to align the source/drain regions exactly to the gate edges. Further, in Type 1 DG-FETs, it is hard to provide a low-resistance, area-efficient contact the bottom gate, since it is buried.

III PROPOSED METHOD

3.1 FINFET Structure Analysis

Type 3 is called as a FinFET because the silicon resembles the dorsal fin of a fish. It is referred to as a quasi-planar device (3D schematic diagram in Fig: 3.8). [14]In the FinFET the silicon body has been rotated on its edge into a vertical orientation so only source and drain regions are placed horizontally about the body, as in a conventional planar FET. The separate biasing in DG device easily provides multiple threshold voltages

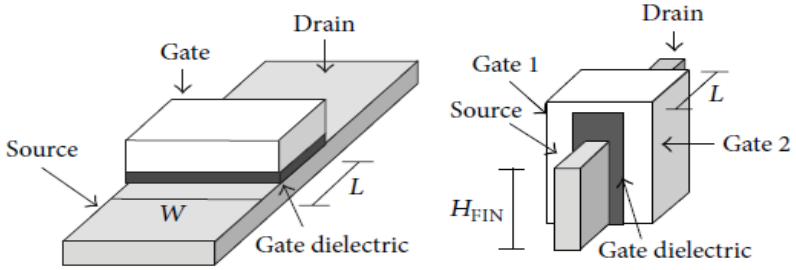


Fig.3.1 Planar MOSFET & FinFET

A gate can also be fabricated at the top of the fin, in which case it is a triple gate FET. The width of a FinFET is quantized due to the vertical gate structure. The fin height determines the minimum transistor width (*Wmin*). With the two gates of a single-fin FET tied together, W_{min} is

$$W_{min} = 2 \times H_{fin} + T_{fin} \qquad (3.1)$$

$H_{fin.}$ is the height of the fin and T_{fin} is the dominant component of the transistor width since T_{fin} is typically much smaller than $H_{fin.}$ Since H_{fin} is fixed in a FinFET technology, multiple parallel fins are utilized to increase the width of a FinFET. The total physical transistor width (W_{total}) of a tied-gate FinFET with *n* parallel fins is:

$$W_{total} = n \times W_{min} = n \times (2 \times H_{fin} + T_{fin}) \qquad (3.2)$$

FinFETs are designed to use multiple fins to achieve larger channel widths. Source/Drain pads connect the fins in parallel. As the number of fins is increased, the current through the device increases [8].

Main features of FinFET are follows:

(1) Ultra thin Si fin for suppression of short channel effects

(2) Raised source/drain to reduce parasitic resistance and improve current drive

(3) Gate last process with low V_T, high k gate dielectrics

(4) Symmetric gates yield great performance,but can built asymmetric gates that target V.

The two vertical gates of a FinFET can be separated by depositing oxide on top of the silicon fin is shown in Fig: 3.1, thereby forming an independent-gate FinFET.

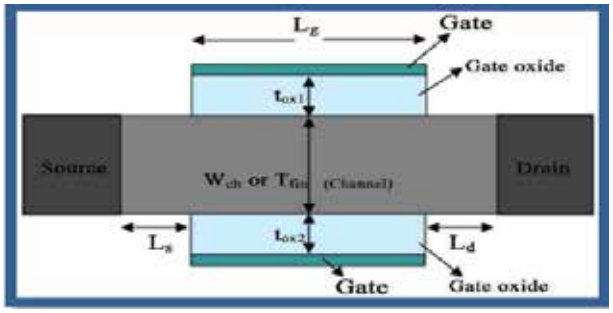


Fig.3.2 Independent-Gate FinFET

3.2 Construction of FinFET

The basic electrical layout and the mode of operation of a FinFET do not differ from a traditional field effect transistor. There is one source and one drain contact as well as a gate to control the current flow [5]. In contrast to planar MOSFETs the channel between source and drain is billed as a three dimensional bar on top of the silicon substrate, called fin. The gate electrode is then wrapped around the channel, so that there can be formed several gate electrodes on each side which leads to reduced leakage effects and an enhanced drive current. The manufacture of a bulk silicon-based multi gate transistor with three gates (tri gate) is described below.

Construction of a Bulk Silicon-based FinFET

1. Substrate: Basis for a FinFET is a lightly p-doped substrate with a hard mask on top (e.g. silicon nitride) as well as a patterned resist layer.
2. Fin Etch: The fins are formed in a highly anisotropic etch process. Since there is no stop layer on a bulk wafer, the etch process has to be time based.
3. Oxide Deposition: To isolate the fins from each other a oxide deposition with a high aspect ratio filling behavior is needed.
4. Planarization: The oxide is planarized by chemical mechanical polishing. The hard mask acts as a stop layer.
5. Recess Etch: Another etch process is needed to recess the oxide film to form a lateral isolation of the fins.
6. Gate Oxide: On top of the fins the gate oxide is deposited via thermal oxidation to isolate the channel from the gate electrode. Since the fins are still connected underneath the oxide, a high-dose angled implant at the base of the fin creates a dopant junction and completes the isolation.

7. Deposition of the Gate: Finally a highly n+-doped poly silicon layer is deposited on top of the fins, thus up to three gates are wrapped around the channel. one on each side of the fin, and - depending on the thickness of the gate oxide on top - a third gate above. The influence of the top gate can also be inhibited by the deposition of a nitride layer on top of the channel. Since there is an oxide layer on an SOI wafer, the channels are isolated from each other anyway. In addition the etch process of the fins is simplified as the process can be stopped on the oxide easily.

3.3 Three Modes of FINFET

3.3.1 Shorted Gate

The two gates are connected together, leading to a three-terminal device [1]. This can serve as a direct replacement for the conventional bulk-CMOS devices.

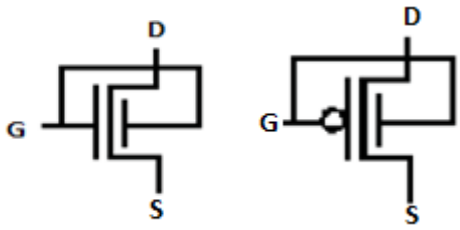


Fig.3.3 Shorted Gate for Both N-Type & P-Type

3.3.2 Independent Gate

The top part of the gate is etched out, giving way to two independent gates [2]. Because the two independent gates can be controlled separately, IG-mode FinFETs offer more design options.

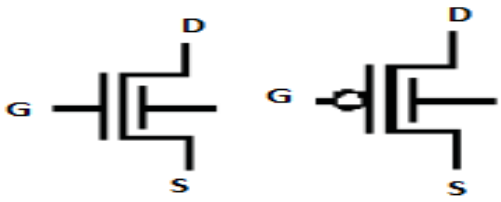


Fig.3.4 Independent-Gate for N-Type& P-Type

3.3.3 Low Power

A low voltage to n-type FinFET and high voltage to p-type FinFET. This varies the threshold voltage of the devices which reduces the leakage power dissipation at the cost of increased delay [1]. A hybrid IG/LP-mode is a combination of LP and IG modes.

3.4 FINFET Logic

3.4.1 Inverter

There are four possible configurations of an INV based on how SG and IG FinFETs are combined to implement them. They are called SG, low-power (LP), IGn, and IGp INV. Their schematic diagrams are shown in Figure 3.22&3.23. As suggested by its name, an SG INV has SG n/p FinFETs. It has a highly compact layout. The other three configurations use at least one IG FinFET. The back-gate of an IG p FinFET (n FinFET) is tied to a VHIGH (VLOW) signal. When these signals are reverse-biased, for example, when VHIGH is 1V above VDD and VLOW is 0 V below ground, there is a significant reduction in Ioff. [1]The presence of an IG FinFET also leads to a more complex layout, resulting in 36% area overhead relative to that of an ×2 SG INV (that is double the size of a minimum-sized SG INV). Table 2 compares the normalized area, delay, and leakage of the various INVs. Clearly, SG INV is the best in area and propagation delay (T p), but incurs much higher leakage current than LP INV. [9] However, LP INV performs poorly in area and propagation delay. IGn INV, however, looks promising based on its intermediate area, delay, and leakage.

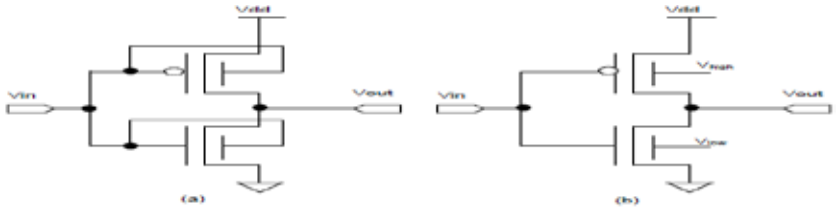


Fig.3.5 FinFET Inverter (a) Shorted gate & (b) Low power gate

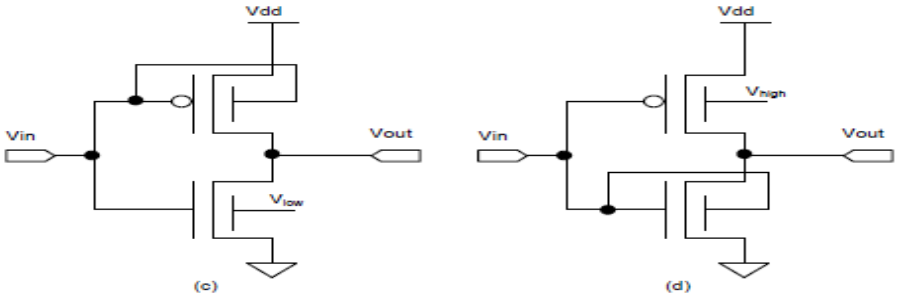


Fig.3.23 FinFET Inverter (c) Independent gate –N Type (d) Independent gate –P Type

3.4.2 NAND

Similar to INVs, NAND2 gates also have SG (LP) configurations in which all transistors are SG (IG) FinFETs. [9] Since there are more transistors in a NAND gate than in an INV, there are more opportunities available for combining SG and IG FinFETs.

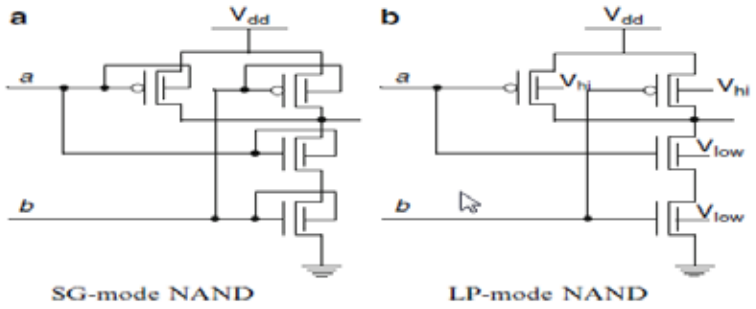


Fig.3.24: FinFET NAND circuit (a) Shorted gate & (b) Low power gate

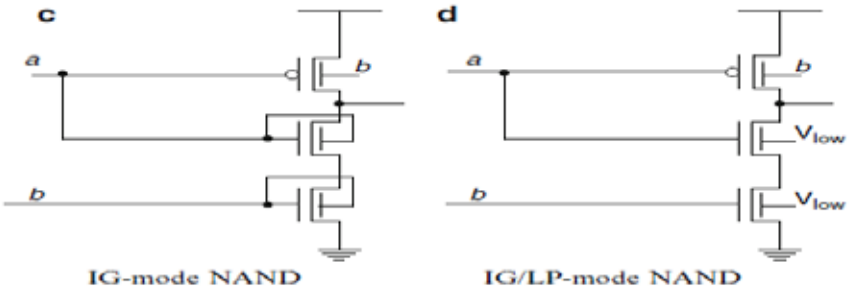


Fig.3.25: FinFET NAND (C) Independent gate & (b) Hybrid mode (IG/LP)

IV. ANALYSIS OF PERFORMANCE CHARACTERISTICS

Table.4.1 Performance Comparison of CMOS & FinFET Inverter

Device	Delay(S)	Power(W)	Bandwidth(G)	Power-Delay Product(PDP)(J)
CMOS	8PS	69µw	16.8G	552AJ
FinFET	7PS	72 µw	18.6G	504AJ

Table 4.1 shows that Performance comparison of CMOS & FinFET Inverter. Analysis describes that compare to CMOS; FinFET has fast switching speed and power delay product also reduced. Leakage also reduced.

Table.4.2 Performance Comparison of CMOS & FinFET NAND

Device	Delay(S)	Power(W)	Bandwidth(G)	Power-Delay

				Product(PDP)(J)
CMOS	26PS	138µw	20G	3.5Fj
FinFET	20PS	134µw	25G	2.7fj

Table 4.2 shows that Performance comparison of CMOS & FinFET NAND. Analysis describes that compare to CMOS; FinFET has fast switching speed and power delay product also reduced. Leakage also reduced.

Table.4.3 Performance Comparison of different modes in FinFET Inverter

Device	Delay(S)	Power(W)	Bandwidth(G)	Power-Delay Product(PDP)(J)
Shorted	7PS	72 µw	19G	504AJ
Low power	13PS	34 µw	11G	442AJ
Independent-P Type	6PS	65 µw	10G	394AJ
Independent-n Type	14PS	55 µw	20G	770AJ

Table 4.3 shows that Performance comparison different modes of FinFET Inverter. Analysis describes that Shorted gate for high performance, Low power gate for greater driving strength, Independent gate for two different signals. Compare to Shorted gate, Low power and Independent gate has low power consumption**.**

Table 4.4 shows that Performance comparison different modes of FinFET Inverter. Analysis describes that Shorted gate for high performance, Low power gate for greater driving strength, Independent gate for two different signals. Compare to Shorted gate, Low power and Independent gate has low power consumption.

Table.4.4 Performance Comparison of different modes in FinFET NAND

Device	Delay(S)	Power(W)	Bandwidth(G)	Power-Delay Product (PDP)(J)
Shorted	20PS	134 µw	25G	2.7f
Low power	30PS	71 µw	20.5G	2.1f
Independent	18PS	83 µw	21G	1.4f
Independent/LP	28PS	68 µw	21G	1.9f

V. CONCLUSION

FinFET is a promising substitute for bulk CMOS for meeting the challenges being posed by the scaling of conventional MOSFETs. Due to its double-gate structure, it offers innovative circuit design styles. Logic gates are implemented in SG-, LP-, IG-, and IG/LP-mode of FinFET. FinFET offer faster switching speed and reduces the leakage current. Logic gates net lists are simulated using HSpice simulator. From the simulation result propagation delay, power consumption, bandwidth, and power delay product can be obtained. The future work will address the implementation of Adder circuit and memory device using FinFET because of its high performance.

REFERENCES

[1]. Ajay N.Bhoj and Niraj K.Jha, "Design of Logic Gates and Flip-Flops in High-Performance FinFET Technology" VLSI, IEEE Transactions on Volume:21

[2]. A. Muttreja, N. Agarwal, and N. K. Jha, "CMOS logic design with independent gate FinFETs," in Proc. Int. Conf. Computer Design, Oct. 2007, pp. 560–567.

[3]. Animesh Datta,Ashish Goal ,"Modeling & circuit synthesis for independently controlled double gate FinFET devices" IEEE Transcation, VOL 26,NO 11,2007

[4]. Dipanjan Sengupta and Resve Saleh ,"Generalized power-delay metrics in deep submicron cmos design",IEEE transaction ,VOL 26,2007.

[5] D. Bhattacharya and N. K. Jha, "FinFETs: From Devices to Architectures" Volume 2014

[6] E.J.Nowak, I.Aller, T.Ludwig, K.kim, R.V.Joshi, "Turning silicon on its edge (double gate cmos/FinFET technology)",IEEE transaction ,VOL 23,2004

[7] International Technology Roadmap For Semiconductors 2007 Edition Emerging Research Materials"

[8] J. P. Colinge, FinFETs and other Multi-Gate Transistors Springer, 2007.

[9] Lu.Z and J. G. Fossum, "Short-Channel Effects in Independent-Gate FinFETs," IEEE ELECTRON DEVICE LETTERS, vol. 28, no. 2, February 2007.

[10] Mohammad Yousefarei,"modeling symmetrical independent gate finfet using predictive technology model"IEEE transaction, 2013

[11] M. Rostami, and K. Mohanram, "Dual Vth independent gate FinFETs for low-power logic circuits," IEEE Trans. CAD of Int. Circuits and Systems, vol. 30, no. 3, March 2011.

[13] Predictive Technology model website Yu (Kevin) Cao, "Nano scale integration and modeling" (www.ptm.asu.edu)

[14] Roy K, Mukhopadhyay, S. ; Mahmoodi-Meimand, H. 2003,"Leakage current mechanisms and leakage reduction techniques in deep-submicrometer cmos circuits" IEEE transaction VOL 91,2003.

[15] Vaidy Subramanian, Bertrand Parvais, Jonathan Borremans, Abdelkarim Mercha," Planar Bulk MOSFETS versus FinFETs," IEEE TRANSACTIONS ON ELECTRON DEVICES, VOL. 53, NO. 12, 2006

BIOGRAPHICAL NOTES

MS.G.SARANYA is presently pursuing M.E final year in Electronics and Communication Engineering Department (specialization in VLSI design) from Theni Kammavar Sangam College of Technology, Theni, Tamilnadu, India.

MS.S.JAKKAMMAL@MALARVIZHI is presently pursuing M.E final year in Electronics and Communication Engineering Department (specialization in VLSI design) from Theni Kammavar Sangam College of Technology, Theni, Tamilnadu, India.

MS.K.KALARANI is working as an Assistant Professor in Electronics and Communication Engineering Department, from Theni Kammavar Sangam College of Technology, Theni, Tamilnadu, India.

GENERATING TERNARY SIMPLEX CODES ARISING FROM COMPLEX HADAMARD MATRICES

Chandradeo Prasad

Assistant Professor, Department. Of CSE, RGIT, Koderma, (India)

ABSTRACT

In this paper, simplex codes are constructed from Hadamard Matrices by compromising on the length of code words. Ternary simplex codes with 2n + 1 words each of length (2n+1) is constructed from certain complex Hadamard matrices. A simplex code of Max type with (4n+1) words each of length 4n is constructed from a Hadamard matrix of order 4n and a discrete Fourier transform matrix of order (4n+1).

Abbreviations: *H-matrix = Hadamard matrix, DFT = Discrete Fourier Transform, BH = Butson Hadamard matrix*

I. INTRODUCTION

At first the following terms are defined and discussed:

1.1 Hadamard matrix

An n x n matrix H with entries ± 1 is called a Hadamard matrix if it satisfies $HH^T = nI_n$, where I_n is the unit and H^T stands for transpose of H. It is well known that for $n \geq 4$, whenever an H-matrix exists, n = 4t. It is conjectured that an H-matrix exists for every order n = 4t. H is called a skew H-matrix. $H - I_n$ is skew in usual sense.

1.2 Complex H-matrix

An n x n matrix H whose entries are complex numbers of the form $e^{i\theta}$ is called a complex H-matrix if it satisfies $HH^+ = n I_n$, where H^+ stands for Hermitian conjugate of H.

1.3 Butson H-matrix

A complex H-matrix is called a Butson H-matrix if it contains a primitive m^{th} root of unity and its powers only. It is denoted as BH (m, n), if n is the order of matrix. A Butson H-matrix BH (m, n) is called a Discrete Fourier Transform (DFT) matrix F (m) if it is of the form F(m)=

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & a & a^2 & \dots & a^{m-1} \\ 1 & a^2 & a^4 & \dots & a^{2(m-1)} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a^{m-1} & a^{2(m-1)} & \dots & a^{(m-1)^2} \end{pmatrix}$$

where $a = e^{2\pi i/m}$

1.4 Simplex code

Let A = {e_1, $e_{2...}$ e_n} be the set of real vectors. Let e_j, e_k stands for the scalar product of the vectors $e_j$and e_k. If $e_j.e_j$ = 1, j = 1, 2, ……..……n and $e_j.e_k$ = -1/(n-1) for 1 $\leq$ (j+k) $\leq$ n, then the set A is called a simplex code. A simplex code is called binary if the elements of the vector e_i belong to a set of two symbols and ternary if the elements belong to a set of three symbols.

A simplex code with (n+1) words of length n, containing at least n real numbers will be called a Max type simplex code.

II CONSTRUCTION ALGORITHMS

2.1 Algorithm I

Input: Given a real H- matrix H = [h_{ij}] of order 4n

Output: A complex H-matrix H* with the following property

$h^*_{jk}=h_{jk}$if $h_{jk}= h_{(4n-j+1)k}$

ih_{jk}, if $h_{jk}= - h_{(4n-j+1)k}$

To prove, let c_k and c_k* be the k^{th}column of H and H* respectively. Then $c_j.c_k = c_jc_k$is the scalar product of $c_j$and c_k. If c_j^Tstands for the Hermitian Transpose of the matrix and c_k is the complex conjugate of c_k then it is sufficient to show that

$$C*_j^+ \; c*_k^- = C_j^+ c_k^-$$

Step 1: We have

$$C*_j^+ \; C*_k^- = \sum_{p=1}^{2n} (h^*_{pj} \, h^*_{pk} + h^*_{(4n-p+1)} h^*_{(4n-p+1)k})$$

Step 2: For each of the four choices arising from

$h_{pj} = \pm h_{(4n-p+1)j}$

$h_{pk} = \pm h_{(4n-p+1)k}$

it can be verified that

$$h^*_{pj} h^{-*}_{pk} + h^*_{(4n-p+1)} h^{-*}_{(4n-p+1)k}$$

$$= h_{pj}h_{pk} + h_{(4n-p+1)j} \, h_{(4n-p+1)k}$$

Hence

$$C*_j^+ \; c*_k^- \quad = C_j^+ c_k^-$$

2.2 Algorithm II

Input: Given a real H-matrix of order 4n

Output: A Max- type Simplex code with (4n + 1) words each of length 4n.

Step 1: Use the result of the algorithm 1 where H* is a complex Hadamard matrix and

$h^*_{jk}=h_{jk}$ if $h_{jk}= h_{(4n-j+1)k}$

ih_{jk}, if $h_{jk}= - h_{(4n-j+1)k}$

Step 2: Let F_1 be a (4n +1) x 4n matrix obtained by deleting the first column of the Fourier Transform matrix F(4n + 1).

Step 3: Let the required ternary simplex codes are the rows of the matrix $C = (1/4n) F_1 H^*$.

Step 4: Now

$$CC^+ = 1/(4n)^2 F_1 F_1^+ (4nI)$$

$$= I - (1/4n)(J - I)$$

Where I is the 4n x 4n unit matrix and J is all I matrix of order 4n.

This establishes the algorithm.

2.3 Example

From the H- matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

We get the matrix

$$1/4 \begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^2\alpha^3\alpha^4 & \alpha^2\alpha^4 & \alpha^3 \\ \alpha^2\alpha^4 & \alpha & \alpha^3 & \alpha^4\alpha^2 \\ \alpha^3 & \alpha^4\alpha^3\alpha^2 & \alpha & \alpha \end{pmatrix} \begin{pmatrix} 1 & i & i & 1 \\ 1 & i & -i & -1 \\ 1 & -i & i & -1 \\ 1 & -i & -i & 1 \end{pmatrix}$$

Where $\alpha = e^{2\pi i/5}$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ -\frac{1}{4} & -sin3\theta cos\theta & cos3\theta sin\theta & sin\theta sin3\theta \\ -\frac{1}{4} & -cos3\theta sin\theta & -cos\theta sin3\theta & -sin\theta sin3\theta \\ -\frac{1}{4} & sin\theta cos3\theta & sin3\theta cos\theta & -sin\theta sin3\theta \\ -\frac{1}{4} & sin3\theta cos\theta & -sin\theta cos3\theta & sin\theta sin3\theta \end{pmatrix}$$

Where $\theta = \pi/5$

The rows of the above matrix is the ternary simplex code.

III. CONCLUSION

This paper shows that the ternary simplex codes with (4n + 1) words of length 4n can be constructed from the known skew symmetric H-matrices for the following values of 4n:

1. $2^t\pi\ k_i$ where t and k_i are positive integers and $(k_i - 1)$ is prime of the form (kt + 3).
2. $(p -1)^u + 1$, where p is the order of a skew Hadamard matrix, $u > 0$ is an odd integer.
3. $2(q +1)$, where $q \equiv 5(\text{mod } 8)$ is a prime power.
4. $2(q +1)$, where $q = p^t$, $q \equiv 5(\text{mod } 8)$ is a prime and $t \equiv 2(\text{mod } 4)$.
5. $4(q + 1)$, where $q \equiv 9(\text{mod } 16)$ is a prime power.
6. $4(q^2 + q+ 1)$, where q is a prime power and $q^2 + q + 1 \equiv 3$, 5 or 7(mod 8) is prime or $2(q^2 + q + 1) + 1$ is a prime power.
7. 4m, where m is any odd number between 3 and 25 inclusive.

If (4t + 1) is a prime power, using algorithm II, we can construct a max – type ternary simplex code with (4n + 1) words each of length 4n from any H-matrix of order 4n.

REFERENCES

[1]. Arasu K.T., Leung, K.H., Ma S.L., Nabav A and Choudhary D. K. R. (2006) "Circulanant Weighing Matices of weight 2^{2t}, Journal of Designs, Codes and Cryptography, Springer Neitherlands, Vol. 41, Number 1/October,2006, pp – 111-123.

[2]. Arasu K.T., W. de Launey and S. L. Ma "On circulant complex Hadamard matrices, Designs, Codes and Cryptography,. 25(2002),123-142.

[3]. Butson A T, Generalized Hadamard Matrices, Proc. Amer. Math.Soc.,13(1962), 894-898.

[4]. Craigen R and HKharaghani, Hadamard Matrices from weighing matrices vis signed groups, Des. Codes, Cryptography, 12(1997), 49-58.

[5]. Craigen R and W D Wallis, Hadamard Matrices, 1893-1993, Congr. Numer. 97(1993), 99-129.

[6]. Golomb S W and G Gong, Signal design for good correlation(2005), Cambridge university press, New York.

[7]. Hedayat A S, N J S Sloane and J Stufken, Orthogonal arrays, Theory and Applications, Springer, New York, 1999.

[8]. Koukouvinos C and Stalianou S "On Skew Hadamard Matrices", Descrete Mathematics, V 308, 13, 2008, 2723-31.

[9]. Mare Gysin and Jennifer Seberry, Construction Methods for weighing matrices of order 4n and weight 4n-2, 2n-1 and n using elementary properties of cyclotomy, In Conference on Combintorial Mathematics and Combinatorian Computing, University of Technology, Aukland, July,1994.

[10]. Mare Gysinand JenniferSeberry, New Weighing Matrices through Linear Combinations of generalized cosets, In Conference on Combintorial Mathematics and Combinatorian Computing, University of Technology, Sydney, July,1996.

[11]. Craigen R, The Structure of weighing matrices having large weights, Spriger, Netherlands, Vol. 5, Number 3, May, 1995.

[12]. Berman G, Families of generalized weighing matrices, Canadian J. Math., 30(1978), pp. 1016-1028.

[13]. Seberry Jennifer, Yamada M, "On product of Hadamard Matrices, Williamson Matrices and other orthogonal matrices using M- Structures", JCMCC 7?(1990), pp. 97-137.

[14]. Seberry Jennifer, Yamada M(1992), " Hadamard Matrices, sequence and block designs, John Wiley and Sons Inc. pp. 431-437.

[15]. Seberry Jennifer, Website: http//www.uow.edu.au/jennie/.

[16]. David E Goldberg, „Genetic algorithms in search, optimization and machine learning", Addision- Wesley Pub.Co.1989.

[17]. C.E.Shannon, "Communication Theory of Security System",Bell,System Technical Journal, 28, 1949

[18]. A.J.Bagnall, "The Applications of Genetic Algorithms in Cryptanalysis", School of Information Systems, University Of East Anglia, 1996.

[19]. N.Koblitz , „A Course in Number Theory and Cryptography", Springer-Verlag, New York, Inc., 1994.

[20]. Menzes A. J., Paul, C., Van Dorschot, V., Vanstone, S. A., "Handbook of Applied Cryptography", CRS Press 5th Printing; 2001.

[21]. National Bureau Standards, "Data Encryption Standard (DES)," FIPS Publication 46; 1977

[22]. Tragha A., Omary F., Mouloudi A.,"ICIGA: Improved Cryptography Inspired by Genetic Algorithms", Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.

[23]. SpillmanR,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substitution Cipher" Cryptologia, Vol.17, No.4, pp. 367- 377, 1993.

[24]. SpillmanR,"Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, Vol.17, No.4, pp. 367-377, 1993.

[25]. Garg Poonam, Genetic algorithm Attack on Simplified Data Encryption Standard Algorithm, International journal Research in Computing Science, ISSN1870-4069, 2006.

[26]. Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B,Jan 2006. 2nd National Conference in Intelligent

Computing & Communication Organized by Dept. of IT, GCET, Greater Noida, INDIA. ISBN: 9788175157538

[27]. L. Ljung, System Identification - Theory for the User. Prentice-Hall, N.J. 2nd edition, 1999.

[28]. J. Schoukens and R. Pintelon, System Identification. A Frequency Domain Approach, IEEE Press, New York, 2001.

[29]. T. Söderström and P. Stoica, System Indentification, Prentice Hall, Enhlewood Cliffs, NJ. 1989.

[30]. P. Eykhoff, System Identification, Parameter and State Estimation, Wiley, New York, 1974.

[31]. A. P. Sage and J. L. Melsa, Estimation Theory with Application to Communications and Control, McGraw-Hill, New York, 1971.

[32]. H. L. Van Trees, Detection Estimation and Modulation Theory, Part I. Wiley, New York, 1968.

EFFECTIVE SECURE MINING OF ASSOCIATION RULE WITH SUBGROUP DISCOVERY IN HORIZONTALLY DISTRIBUTED DATABASES

[1]K. Sindhika, [2]P. Ganesh Kumar,

[1]PG Scholar, [2]Assistant Professor,
Department of Information Technology,
Anna University Regional Centre, Coimbatore (India)

ABSTRACT

Data mining can extract important knowledge from large data collections – but sometimes these collections are split among various parties. In Privacy concerns leakage of information can be tackled by using cryptographic techniques namely AES. The methods incorporate cryptographic techniques to minimize the information shared, it may reduce the performance of mining task. Subgroup discovery concept has been enforced to bring top k pattern for faster mining.It finds patterns in the coupling of the databases, without discovering the local databases.

Indexterms : Secure Mining, Subgroup Discovery, Frequent Itemsets, Association Rule.

I INTRODUCTION

In Data mining, association rule is a popular and well researched method for discovering interesting relationsbetween variables in large databases. Piatetsky-Shapiroillustrates observation made on strong rules discoveredin databases using different measures of interestingness and presented accordingly.Agrawal et al introduced association rules for discovering regularities between products in large scale transaction data recorded by point-of-sale (POS) systems in supermarkets through founded strong rules. For example, the rule Found in the sales data of a supermarket would indicate that if a customer buys coffee powder and milk together, there is possibility of buying sugar.These information can be retrieved for decision making in markets for e.g., product placements. In summation to the above example from market basket analysis association rules are utilized today in many application fields including Web usage mining, intrusion detection and Bioinformatics [5].

The two significant basic measures of association rules are support(s) and confidence (c). Support(s) is defined as the proportion of records that contain X unionY to the overall records in the database. The total for each item is augmented by one, whenever the item is crossed over in different transaction in the database during the course of the scanning.Confidence (c) is determined as the ratio of the number of transactions that contain X union Y to the overall records that contain X. Association rule mining is to find out association rules that satisfy the predefined minimum support and confidence from a given database. If the value of support and confidence are minimum then the association rule is said to be stronger.

The Application ofAssociation rule mining in market basket analysis is

- To observe the point of sales transaction.

- From uses information on what customers buy to provide insights into who they are and why theymake certain purchases.
- To predict the product that occurs together.

Subgroup discovery is a method to identify relations between a dependent variable (target variable) and independent variables. For example, consider the subgroup described by ”smoker=true AND family history=positive” for the target variable coronary heart disease=true. Subgroup discovery does not necessarily focus on finding complete relations; instead partial relations, i.e., (small) subgroups with ”interesting” characteristics can be sufficient. The discovered subgroup patterns must essentially satisfy two conditions.

i. Interpretable for the analyst
ii. It should be interesting with respect to the criteria of the user.

Where the Interestingness is typically defined by a quality function, which can take certain statistical or other user-defined quality criteria into account. Interestingness rely on the characteristics of the user’s choice.

II RELATED WORK

Secure Mining of Association Rules in Horizontally Distributed Databases:A novel protocol UNIFI-KC (Unifying lists of locally Frequent Item sets— Kantarcioglu and Clifton) is based on the Fast Distributed Mining (FDM) Algorithm which is an unsecured distributed version of the Apriori algorithm [1]. The main ingredients in our protocol are two novel secure multi-party algorithms - one that computes the union of private subsets that each of the interacting players hold, and other that checks for the inclusion of an element held by one player in a subset held by another. It offers enhanced privacy with respect to the protocol. It is also simpler and significantly more efficient in terms of communication rounds, communication and computational cost.

A Fast Distributed Algorithm for Mining Association Rules: Fast Distributed Mining of association rule which generates a small number of candidate sets and substantially reduces the number of messages to be passed at mining association rules. The FDM algorithm proceeds as follows: (i) Initialization, (ii) Candidate sets generation, (iii) Local Pruning, (iv) Unifying the candidate item sets, (v) Computing local supports and (vi) Broadcast Mining Results. Main discussion made on two issues first one about the relationship between the effective FDM and distribution of data and another one deals with the support threshold relaxation for possible reduction of message overheads. Some interesting properties between global and local large itemsets are observed. Two powerful pruning techniques are proposed namely global pruning and local pruning which could improve the computation speed at data mining preprocessing task [3].

Privacy Preserving Association Rule Mining in Vertically Partitioned Data :Here the problem of Association Rule Mining where the transaction are distributed across sources were discussed. The two-party algorithm used for efficiently discovering frequent itemsets with minimum support levels, without revealing individual transaction values from either site. By vertically partitioned, each site contains some elements of a transaction. Using the traditional “market basket” example, one site may contain clothing purchases , while another has grocery purchases. Using a key such as credit card number and date, join these to identify relationships between purchases of clothing and groceries. However, this discloses the individual purchases at each site, possibly violating consumer privacy agreements. Other problem is to mine association rules across two databases, where

the columns in the table are different sites, splitting each row. One databases is designated the primary and it is the initiator of the protocol. The other databases is the responder. There is a join key present in both databases. The other remaining attributes are present in any onedatabases, but not both. The goal is to find association rule involving attributes other than the join key. Finally, it is necessary to quantify the accuracy and the efficiency of the algorithm, in view of the security restrictions.

Privacy-preserving Distributed Mining of Association Rules on Horizontally Partitioned Data :The overview of Privacy Association Rule Mining has been outlined. The two phases are discovering candidate itemsets and determining which of the candidate itemsets meet the global support/confidence thresholds. The first phase uses commutative encryption where each party carries out encryption for its own frequent itemsets. The encrypted itemsets are then passed to other parties, until all itemsets are encrypted. These are passed to a common party to avoid and eliminate duplicates, and to begin decryption process. These set are then passed to each party, and each party decrypts each itemset. By this cryptographic technique for preventing the leakage of information have been studied [2].

The rest of the paper is organized as follows: In section III the design of the association rule with subgroup discovery is presented and provides the detailed description of modules used in the system. Section IV covers the conclusion part of this paper.

III SYSTEM DESIGN

The system focuses to build an association rule with cryptographic technique as well as rapid mining through the subgroup discovery technique. The modules of the system design include:

- Collecting the everyday transaction of the customer from various super markets and forming homogenous databases for analysis.
- Building a strong association rule with two significance measure namely minimum support and minimum confidence.
- Cryptographic technique is applied for datasets to perform the mining process in secure manner.
- Subgroup discovery technique is utilized for faster mining which brings top k patterns.

The input datasets are collected from marketing field by the point of sale to generate association rule through apriori algorithm. In this algorithm, the candidate key is generated for pruning the unwanted dataset before scanning the entire databases.

The following figure illustrates the overall work flow of the system:

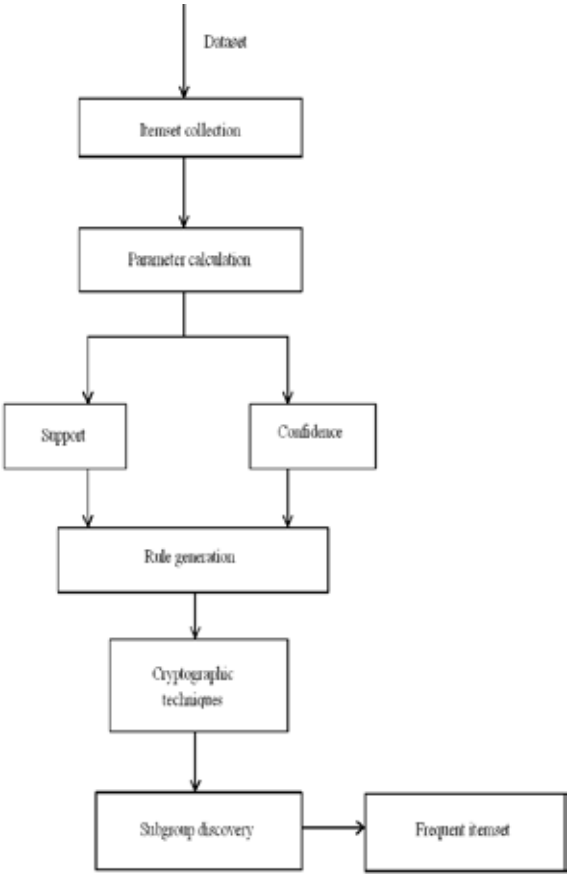


Fig. 1: Architecture Diagram

3.1 Collection of Datasets

Here the datasets refer to the everyday purchase transaction of customer. The system build the homogenous databases (same schema with unique entities) to feed the observed transaction data from the point of sale in various market.

3.2 Association Rule Mining

Association rules are if/then statements that help uncoverrelationships between seemingly unrelated data in a relational database or any other information repository. Anexample association rule "If a customer buysa dozen eggs, he is 80% likely to also purchase milk."By analyzing the data association rules are created forfrequent if/then patterns and using the criteria support andconfidence to identify the most important relationships. Support is an indicating term, it indicates how frequently the items appearin the database. Confidence is an indication of the number of timesthe if/then statements have been found to be true. Some technique used in building the association rule namely Apriori and Fast Distributed Mining Algorithm.

Apriori is designed to operate on databases containing transactions. The Apriori Algorithm is used to findassociations between different sets of data. It is sometimesreferred to as "Market Basket Analysis". Each set of data has a number of items called a transaction. The Apriori algorithm outputs sets of rules that tell us how often items arecontained in sets of data.

The FDM algorithm proceeds as follows:

1. Initialization
2. Candidate Sets Generation
3. Local Pruning
4. Unifying the candidate item sets
5. Computing local supports
6. Broadcast Mining Results

The two parameters for association rule has been calculated by following formula :

$$\text{Confidence} = \frac{\text{Support\_count}(A \cup B)}{\text{Support\_count}(A)}$$

3.3 Advanced Encryption Standard

AES is not exactly Rijndael where Rijndael supports a larger range of block and keysizes.AES has a fixed block size and has a size of 128-bits and a key size of 128,192,256 bits.AES is a specification for the encryption of electronic data established by the U.S National Institute of Standard and Technology(NIST) in 2001.

For analyzing the structure and design of new AES ,the following three criteria were used:

- Resistance against all known attacks.
- Speed as well as code compactness on a wide range of platform.
- Design simplicity along with its similarities and dissimilarities and other symmetric ciphers.

AES algorithm is a symmetric block cipher algorithm that can encrypt(encipher)and decrypt(decipher)the information.AES can encrypt data much faster than Triple DES.AES is included in the ISO/IEC 18033-3 standard.AES ismade available in many different encryption packages,and is one of the first publicly accessible and open cipher approved by National Security Agency(NSA) for top secret information.

AES uses 128 bits blocks and key size of 128,192 or 256 bits. It doesn't have fiesel structure and it is block cipher which consists of 10 rounds with four separate functions namely byte substitution, permutation, arithmetic operation and Xor with a key.

The exact transformations occur as follows: each round consists of four steps:

- Add subkey: A portion of a key unique to this round is XOR with the round result. This operation provides confusion and incorporates the key.
- Byte Substitution: It uses S-box structure similar to DES, substituting each byte of a 128-bit block.
- Shift row: It is a simple permutation operation. For 128 and 192 bit block sizes, row n is shifted left circular (n – 1) bytes while for 256-bit blocks, row 2 is shifted 1 byte and row 3 and 4 are shifted 3 and 4 bytes, respectively.
- Mix column: The four bytes of every column are mixed in a linear fashion. This involves shifting left and XOR with the round result. These provide both confusion and diffusion.

The following figure illustrates the round involved in the AES algorithm:

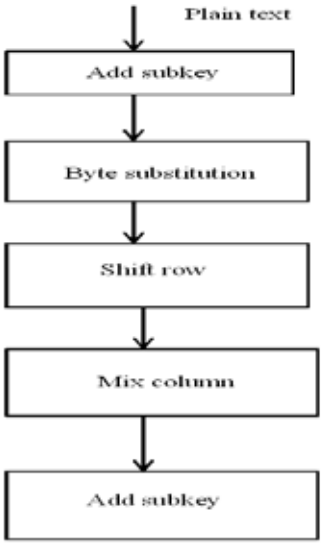


Fig. 2: Round 1 of AES Algorithm

AES has similar operation for both encryption and decryption where the operation get reserved while implementing decryption.

3.4 Subgroup Discovery

A subgroup discovery task mainly relies on the following fourproperties: the target variable, the quality function, the subgroup description language and the search strategy. The target variable (e.g., coronary heart disease) may be binary, nominal or numeric. Depending on its type, there are different analytic questions, e.g., we can search for significant deviations of the mean of a numeric target variable. The description language specifies the individuals from the general population belonging to the subgroup. Subgroup descriptionlanguages can be either single-relational or multi-relational. In the case of single-relational propositional languages a subgroup description can be defined as follows: Let $\Omega_A$the set of all attributes with an associated domaindom(a) of values.V is defined as the (universal) set of attribute values of the form (a = v), $a \in \Omega_A$, $v \in$dom(a) [6].

A quality function measures the interestingness of the subgroup mainly based on a statistical evaluation function, such as the the chi-squared statistical test. It is used by the search method to rank the discovered subgroups during search. Then, quality functions can be used to measure the characteristics of the subgroups according to the analytical questions. In the simplest case, one population share is considered, but also several shares (segments) can be used, e.g., segmenting by sex = male vs. sex = female.

Algorithm 1:

INPUT: length limit L and local databases D1,D2.....DS.
Site 1 initiates the secure calculation of |D| and $|D^+|$ and broadcasts the result
site1 creates a local iterator iter and queue Q_1, site S creates a local queue Q_S
whilehasnext(iter)do
site1 calculate and broadcasts S_i=next(iter)
site1 generates a random number r_i uniformly in [0,....M], enqueuesr_i in Q_1,adds its local support (|D1+[Si]|(1-P0)-|D1-[Si]|$P0^{\cdot}$|D| to $r_i$and sends the result(mod M)to site2
sites 2.....s-1 add their local support to the intermediate sum and send the result (mod M)to the next site

site S adds its local support to the sum and enqueues the result,$q_i + r_i$(mod M),in Qs
end while
while Q1 contains more than 1 value *do*
site 1 dequeuesr_α and r_β from Q_1,generates a random number r' uniformly in [0,....M]and enqueues r' in Q_1
site1 generates and encrypts a circuit that computes(max(q_α,q_β)+r')modM) from.It sends the circuit to siteS together with the cryptographic keys corresponding to the input bits for r_α,r_β and r'
site1 sends the encoding table for the remaining inputs to site T
site S dequeues(r_α+$q_{\alpha'}$) and (r_β+$q_{\beta'}$)from Qs, asks site T for the corresponding cryptographic keys, evaluates the encrypted circuit and enqueues the result,(r'+max(q_α,q_β)modM)in Qs
end while
site 1 and S calculate $q_{max}$by exchanging the two remaining values
for every subgroup descriptions Si do
if q_i'+$r_i \geq r_i$+$_{qmax'}$|D| then return ‹si,qmax›
end for

IV CONCLUSION

Thus the subgroup discovery improves the performance of Association rule in horizontally distributed databases which brings top k pattern which leads to rapid mining. It also eliminate the duplicate item set. AES helps in preserving the confidential information of the organization. By this association rule mining can be built more strongly.

REFERENCES

[1] TamirTassa,"Secure Mining of AssociationRules in Horizontally Distributed Databases," IEEE trans. Knowledge and Data Eng., vol.26, no.4, pp.970-98, April 2014.

[2] M. Kantarcioglu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 9, pp. 1026-1037, Sept. 2004.

[3] D.W.L. Cheung, J. Han, V.T.Y. Ng, A.W.C. Fu, and Y. Fu, "A Fast Distributed Algorithm for Mining Association Rules," Proc. Fourth Int'l Conf. Parallel and Distributed Information Systems (PDIS), pp. 31-42, 1996.

[4] J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge discovery and Data Mining (KDD), pp. 639-644, 2002.

[5] Y. Lindell and B. Pinkas, "Privacy Preserving Data Mining," Proc. Crypto, pp. 175-186, 2005.

[6] H. Grosskreutz, B. Lemmen, and S. Ruping, "Secure Distributed Subgroup Discovery in Horizontally Partitioned Data," Trans. Data Privacy, vol. 4,no. 3,pp. 147-165,2011.

SUSTAINABILITY ASSESSMENT OF INFRASTRUCTURE PROJECTS

Madhuri Reddy[1], Rahul S.Patil[2]

[1]Post graduate student, [2]Assistant Professor, Department of civil Engineering,
Dr.D.Y.Patil Institute of Engineering & Technology, Pimpri, Pune, Maharashtra, (India)

ABSTRACT

Sustainability of an Infrastructure project is governed by a wide range of parameters and indicators .These indicators should represent the overall sustainability of the infrastructure projects. Hence there is a need to identify the sustainability indicators .The approaches available so far focus mainly on some aspects of the sustainability of the project .This paper defines and identified the essential indicators which can be grouped under the Economic, Environment and Technical heads of sustainability. The paper is based on a wide literature survey of the previous research work done in the field. A set of key assessment indicators were identified for assessing the overall sustainability of infrastructure projects.

Keywords: Environment, Indicators, Infrastructure, Sustainability.

I. INTRODUCTION

Sustainable development or the concept of sustainability is fundamental to almost all kinds of human activities .Human development is synonymous with infrastructure development .The term infrastructure include a wide range of services like power, telecommunication ,water supply ,sanitation and solid waste disposal and collection, roads ,dams ,railways ,urban transportation, ports, airports[1].During the past five decades more than 30% of the world bank's investments were in developing countries for infrastructure projects. Hence assessing and forecasting of sustainability of infrastructure projects is of great consequence in decision making for sustainable development.[2],[3].The sustainability assessment of infrastructure projects requires a combined approach of environmental ,economic and technical services. Several researchers have analyzed infrastructure sustainability from different perspectives .among the available sustainability assessment methods the sustainability assessment indicators approach has proved to be most transparent ,consistent and useful method in decision making process [4].No method adopts the dimensions of sustainability .This has been a motivation for the study to arrive at a list of key assessment indicators that incorporated all the elements of sustainability and sustainable performance of infrastructure projects.

II.LITERATURE REVIEW

Several researchers address models/frameworks for defining sustainability.Venegas proposed that sustainability is comprised of inter related systems i.e. financial, environmental and ecological [5]. Some researchers have grouped the sustainability parameters into three key categories: Economical, social and environmental. By using the key assessment indicators the sustainability of an infrastructure project can be assessed by giving a

sustainability score. This could help decision makers find an optimal solution among the available alternatives which could give a maximum sustainability score [6]. Indicators are becoming increasingly recognized as an important tool in understanding infrastructure sustainability .The Indicators can help in decision making process based on measurable conditions and results. Indicators approach of assessing an infrastructure project is not a substitute for exercising judgment in infrastructure decision making but an effective tool in decision making[7].The sustainability assessment methods are a planning tool. Indicators should have appropriate parameters that should make assessment possible. Every project may be evaluated in terms of environmental and technical aspects of sustainability where integration and optimal balance of all the three dimensions and objectives is needed for overall sustainability.

Mehmet A.Boz et al. had developed three innovative system based bench marks to assess civil infrastructure projects; namely work ,nature and flow. They proposed a three step methodology compromising of survey development, data collection and analysis [8].

The research conducted by Melissa M.Bilec et al , says that though much of the assessment attention lies on the environmental effects some methods focus on aspects like energy use hazardous material indoor climate and sick building syndrome [9].

III.BACKGROUND

3.1 Construction Industry

It is one of the clusters of consumption of mankind that places the maximum burden on the environment. In order to understand the construction process from an environmental perspective the effects of built environment on natural environment have to be studied. The construction process should also be evaluated with a multi disciplinary frame work which would lead to sustainable development.

3.2 Sustainability

The word sustainable development was first introduced in the report of the World Commission on Environment and Development in 1987[10].Sustainable development has three basic dimensions (1) Economic (2) Environmental (3) social ([11].Initially the concept of sustainability was only restricted to the environmental aspect. As the concept gained momentum the other dimensions like social, cultural and economic sustainability gained attention. These interdependent dimensions of sustainability are what constitute the overall sustainable development.

The most evident effect of urbanization and infrastructure development are the division of the land into smaller units, the pattern of land use and the intensity of the land use. Hence the concept of sustainable development finds its place in order to improve the social structure, economic development and higher standard of living for all people. For rough understanding of sustainability the following four aspects can be defined.

3.2.1. Technical Sustainability: It refers to the design, scientific research and technology, ease and efficiency of durable construction, safe operation, material selection ,reduction, recovery, reuse of construction material.

3.2.2. Environmental sustainability: Focuses on the effect of the engineering process, the structures and the material on the environment.

3.2.3. Economic sustainability: This refers to the profit making policies. Economic health of communities. The impact of the structures on the economic health, employment and the standard of living.

3.3 Sustainability Assessment

Several researchers have studied Infrastructure Sustainability from different perspectives. Rackwitz et al , proposed a maintenance strategy for improvement of the effectiveness of a project based on cost benefit analysis[12].Assa Amiril et al, proposed a relationship between sustainability factors and performance for Malaysia Railway infrastructure projects[13].Paolo Bocchini et al, developed a unified approach of Resilience and sustainability[14]. Liyen Shen et al, provided an alternative solution for assessing sustainability by introducing Key Assessment Indicators using Fuzzy set theory[15].

IV. ASSESSMENT INDICATORS

4.1 Economic

It is the statistics about an economic activity. Economic indicators allow analysis of economic performance and predictions of future performance.

4.1.1 Capital Cost: Capital costs are fixed, one-time expenses incurred on the purchase of land, construction equipment, and cost of construction of an Infrastructure Project. It is the total cost needed to bring a project to a commercially operable status.

4.1.2 Life cycle cost: Sum of all the recurring and onetime costs over the full life span of the structure or the project.

4.1.3 Financial returns: The gain or loss of a security in a particular period. The return consists of the income and the capital gains relative on an investment. It is usually quoted as a percentage.

4.1.4 Improvement of regional economy: The way in which the proposed Infrastructure project would affect the economy of the region.

4.1.5 Affordability: This parameter indicates the feasibility of the project in terms of the available finances

4.1.6 Payback period: Payback period in capital budgeting refers to the period of time required to recoup the funds expended in an investment, or to reach the break-even point. The time value of money is not taken into account.

4.2 Technical Sustainability

Refers to the ability to keep the project running with minimum down time.

4.2.1 Performance: This indicator refers to the performance of the project in terms structural designs, whether the project is suitable for its intended purpose.

4.2.2 Reliability: Refers to the extent to which the project is reliable in serving its intended purpose.

4.2.3 Durability: Refers to the ability of the structure to last for the predetermined period without deterioration.

4.2.4 Vulnerability to failure: Refers to the extent to which the structure is susceptible to failure and damage

4.3 Environmental

4.3.1 Air pollution: Refers to the pollution the proposed project could cause to the air during the construction and operation phase of the project

4.3.2 Water pollution: Refers to the pollution the proposed project could cause to the water bodies and the ground water of the area during the construction and operation phase of the project.

4.3.3 Noise pollution: Refers to the pollution the proposed project could cause to the Noise levels of the surroundings during the construction and operation phase of the project

4.3.4 Waste generation: Refers to the waste generated during the construction phase and the methods of waste disposal

4.3.5 Visual impact: Refers to the aesthetic impact the structure would have on the surroundings

4.3.6 Ecological impacts: Refers to the impact the structure would have on the various ecosystems present in the surrounding areas.

4.3.7 Energy Savings: Refers to the reduction in the consumption of energy from various renewable and non renewable sources and thereby reducing the impact on the environment.

4.3.8 Natural resource utilization: Refers to the extent to which natural resources in the area were utilized without causing negative impact to the environment.

ASSESSMENT INDICATORS

S.No	Group	Indicators
1	Economic	Capital Cost
2		Life Cycle Cost
3		Financial Returns
4		Improvement of Regional Economy
5		Affordability
6		Payback Period
7	Technical	Performance
8		Reliability
9		Durability
10		Vulnerability to Failure
11	Environmental	Air Pollution
12		Water Pollution
13		Noise Pollution
14		Waste Generation
15		Visual Impact
16		Ecological Impacts
17		Energy Savings
18		Natural Resource Utilization

V. APPLICATION

The assessment indicators mentioned above in the table can be circulated among professionals, experts and officials dealing with infrastructure projects to arrive at a score for each of the indicators based on level of significance. The data so obtained can be checked for reliability by calculating the Cronbach's Alfa[6]. A Fuzzy set theory can be proposed to give the sustainability score to the proposed infrastructure project. This can help the decision makers to choose the alternative plans for the proposed Infrastructure project.

VI. CONCLUSION

Infrastructure projects play a major role in Economic, Social and Environmental activities of any country. Therefore before implementation their sustainability performance has to be properly assessed. This study therefore introduces a set of indicators which help in assessing the overall sustainability of a project. The Indicators mentioned above can be used to assess a project by weighed sustainability score .The application of assessment indicators can help decision makers to choose an optimum solution from available alternatives based on the sustainability score

REFERENCES

[1]. World Bank. (1994). World development rep. 1994: Infrastructure for development, Oxford University Press, Oxford, UK, 1–12.

[2]. United Nations Centre for Human Settlements UNCHS. 2001 . Cities in a globalizing world: Global report on human settlements 2001, Earth scan, London.

[3]. Capello, P., and Nijkamp, P. 'In search of sustainable human settlements' Ecologic. Econ., 40 2, 151-155. 2002.

[4]. OCED 2002, participatory decision making for sustainable consumption, policy case study series Paris.

[5]. Vanegas, J. 'Road Map and Principles for Built Environmental Sustainability'. Environment, Science, and Technology. Vol. 37, 2003

[6]. Liyin Shen,Yuzhe Wu,Xiaoling Zhang, 'Key Assessment Indicators for Sustainability of Infrastructure Projects', Journal of Construction Engineering and Management, Vol. 137, No. 6, June 1, 2011,ASCE

[7]. Developing Indicators and Benchmarks' issue no 1.1 publication date April 2003 Federation of Canadian Municipalities and National Research Council

[8]. Mehmet A. Boz and Islam H. El-adaway, 'Managing Sustainability Assessment of Civil Infrastructure Projects Using Work, Nature, and Flow', Journal of construction Engineering and Management, Vol. 30, No. 5, Sept, 2014,ASCE

[9]. Bilec, M. M., Ries, R. J., and Matthews, H. S. (2010b). 'Life-cycle assessment modeling of construction processes for buildings.' Journal of Infrastructure System, Vol. 16, No. 3, Sept, 2010, ASCE

[10]. World Commission on Environment and Development WCED. 1987. Our common future, Oxford University Press, New Delhi.

[11]. Heijungs, R., Huppes, G., and Guinee, J. B. 'Life cycle assessment and sustainability analysis of products, materials and Technologies'. J.PolymerDegrad.Stabil.,vol 95, issue3,March 2010.

[12]. Rackwitz, R., Lentz, A., and Faber, M. (2005). 'Socio-economically sustainable civil engineering infrastructures by optimization.' J.Struct.Saf., vol 27, issue3, July 2005

[13]. Assa Amiril, Abdul Hadi Nawawi, Roshana Takim, Siti Nur Farhana Ab. Latif, 'Transportation Infrastructure Project Sustainability Factors and Performance', Science Direct, Procedia - Social and Behavioral Sciences volume153,16 October (2014)

[14]. Paolo Bocchini.M,Dan M.Frangopol,Dist.M,;Thomas Ummenhofer;and Tim Zinke, 'Resilience and Sustainability of Civil Infrastructure :Towards a Unified Approach' , Journal of Infrastructure systems,vol 20,no2,June2014