ELECTRONICS & COMMUNICATION ENGINEERING

TECH CONNECT

March, 2019

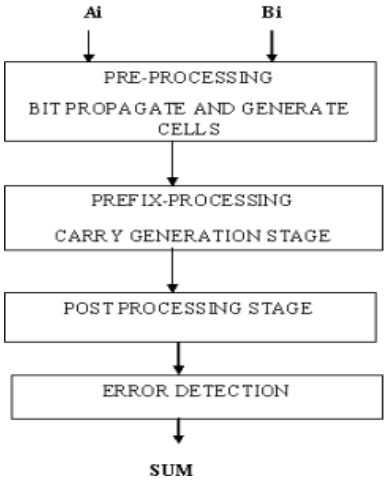
LAKIREDDY BALIREDDY COLLEGE OF ENGINEERING
MYLAVARAM

Contents

1. Parallel Prefix Brent- Kung Adder

Adders are basic functional units in computer arithmetic operations. Binary adders are used in microprocessors for addition and subtraction operations, floating point multiplication and division. Therefore adders are fundamental and basic components, improvement in performance is one of the major challenges in digital designs [1].

Brent Kung adder is used for high performance addition operation, and parallel prefix adder used to perform the addition operation [3].



It is look like a tree structure to perform the arithmetic operations. It consists of black cells and gray cells.[2] Each black cell consists of two AND gates and one OR gate [4]. Each gray cell consists of only one AND gate pi. It denotes propagate and it consists of only one AND gate [5] given in equation 1. gi denotes the generate and it consists of one AND gate and OR gate given in equation 2. [6]

pi= Ai XOR Bi ----(1)

gi= Ai AND Bi ---------(2)

Gi denotes the carry generate and it consists of one AND gate and one OR gate given in equation 3.It is used for first black cell. [8]

Gi=pi OR [gi AND cin] (3)

The Parallel Prefix adders are suitable for VLSI implementation since it differs from other adders, it can be used for large word sizes. The proposed design reduces the number of prefix operation by using more number of Brent-Kung stages and lesser number of Kogge-Stone Stages. This also reduces the complexity, silicon area and power consumption. Parallel Prefix Adder can be subdivided in the following stages: Pre-Processing, Post Processing, Error Detection and Error Correction. The Error

Correction Stage is Off the critical path, as it has two clock cycles to obtain the exact sum when speculation fails. The Pre-Processing and Post-Processing Stages of a Prefix adder involve only simple operations on signals to each bit location.Fig.1. shows the block diagram of Parallel-prefix Adder. Hence, the adder performs mainly on Prefix operation. Therefore black dots represent the prefix operator, and white dots represent the simple place holders.

This also reduces the complexity, silicon area and power consumption. Parallel Prefix Adder can be subdivided in the following stages: Pre-Processing, Post Processing, Error Detection and Error Correction. The Error Correction Stage is Off the critical path, as it has two clock cycles to obtain the exact sum when speculation fails. The Pre-Processing and Post-Processing Stages of a Prefix adder involve only simple operations on signals to each bit location.Fig.1. shows the block diagram of Parallel-prefix Adder. Hence, the adder performs mainly on Prefix operation. Therefore black dots represent the prefix operator, and white dots represent the simple place holders

Parallel-Prefix adders are compute addition in two steps: one is to obtain the carry at each bit, and next one is to compute the sum bit based on the carry bit. Inappropriately, prefix trees are algorithmically slower than fast logarithmic adders, such as the carry propagate adders, however, their regular structures promote excellent results when compared to traditional CLA adders. This happens with in VLSI architectures because a carry-look ahead adder, such as the one implemented in one of Motorola's processors [9], tends to implement the carry chain in the vertical direction instead of a horizontal one, which has a tendency to increase both wire density and fan-in/out dependence. Therefore, although logarithmic adder structures are one of the fastest adders algorithmically, the speed efficiency of the carry-look ahead adder has been hampered by diminishing returns given the fan-in and fan-out dependencies as well as the heavy wire load distribution in the vertical path. In fact, a traditional carry-look ahead adder implemented in VLSI can actually be slower than traditional linear-based adders, such as the Manchester carry adder.

Sudheer Kumar Yezerla et al. [10] investigated different types of 16 bit PPA's which were implemented using Verilog Hardware Description Language. The tool used was Xilinx Integrated Software Environment (ISE) 13.2 Design Suite. The parameters considered for results were an area, power, and delay.

Anas Zainal Abidin et al. [11] investigated the performance of 4-bit BKA using Silvaco EDA tool- 0.18um Silterra Technology. Brent Kung Adder was implemented

using Basic Logic Gates and Compound Gate, and then they simulation study was done by considering the design in different transistors sizes with power consumption, a number of transistors used and propagation delay as parameters.

Pappu P. Potdukhe et al. [12] proposed architecture for carrying Select Adder (CSA) using parallel prefix adder. 4 bit Brent Kung adder was used to design CSA instead of 4 bit Ripple Carry Adder (RCA). Power and delay of 4 bit RCA and 4-bit BKA architecture were calculated. Relative performances of 4 bit RCA and BKA were described using TANNER EDA tool designs.

Kostas Vitoroulis [13] designed a parallel prefix adder which employs 3-stage structure of carrying look-ahead adder. An improvement was introduced in the carry generation stage different architectures for carry generation were presented. Also, the different parallel prefix adder architectures which were developed since the 1950s were presented. PPA's are basically consists of 3 stages. They are: Pre computation, Prefix stage and Final computation .The diagram Fig.2.is shown in below.

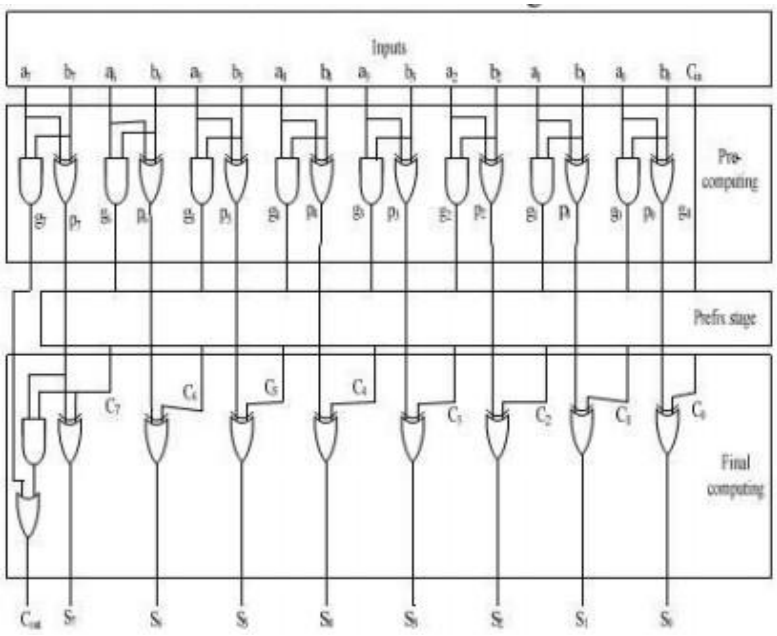


Fig.2.PPA Structure

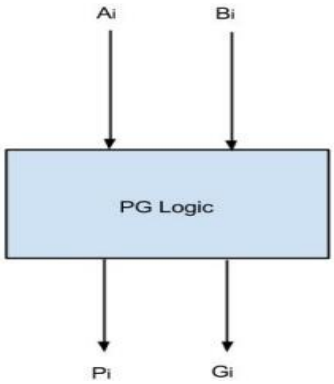
In pre computation stage, propagates and generates are Computed In the prefix stage, the black cell (BC) and gray cell (GC) generates only the building prefix structures. Final computation, the sum and carryout are the final output. Black Cell and Gray Cell In black cell having four inputs and two outputs propagation means and operation and generation means And-or operation.

HAN-CARLSON ADDER WITH ERROR DETECTION AND ERROR CORRECTION:

The conditions wherein at least one of the estimated carries is wrong (mis-prediction) are signed by the error detection stage. In case of mis-prediction, an error signal is emphasised by the error detection stage and the output is post- processing stage is discarded. The error correction stage will give the correct sum in the next clock period. The error correction stage computes the exact carry signals, to be used in case of mis-prediction. The error correction stage is composed by the levels of the prefix-processing stage pruned to obtain the speculative adder.

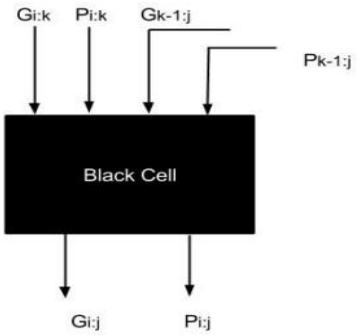
Proposed System

Brent-Kung adder is a very popular and most widely used in adders. Generally, it



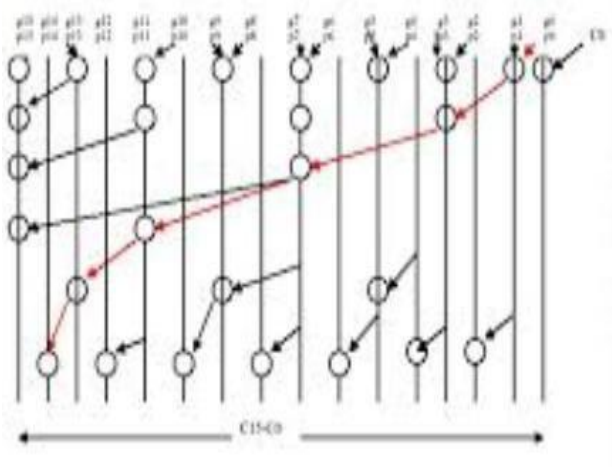
gives an excellent number of stages from input to all outputs but with asymmetric loading of Intermediate stages. It is one of the parallel prefix adders.

The inputs A and B are given to PG logic as shown in the block diagram. 32 PG logic blocks are needed for a 32-bit adder. The outputs of this block are propagate (P) and generate (G) signals. The block diagram shows the fig 6&7.These signals are given to the tree structure of Brent Kung adder. This structure contains grey cells and black cells arranged as discussed in Brent Kung adder section. A grey cell has three inputs and one output as shown in the figure. Generate and propagate signals from present stage and generate signal from previous stage are inputs. Group generate signals is the output. Each stage ends with a grey cell in any tree structure and the output of this grey cell is the group generate signal which is considered as the carry of that stage. Black cell has 4 inputs and 2 outputs. The inputs for a black cell are P and G signals of present stage and P, G signals of previous stage.



Block diagram of Black cell

It is one of the basic adders where these adders are the ultimate class of adders that are depends on the uses to generate and propagate logics. In case of Brent-kung adders the cost, the wiring complexity is less. But the gate level is depth of the Brent-Kung adders is 0 (log2 (n)). In ripple carry adders each bit to wait for the last bit operation. In this parallel prefix adder is instead of waiting for the carry propagation of the initially addition, the idea here is to overlap the carry propagation of the first addition the computation in the another addition, and so forth, since repetitive additions will be performed by a multi-operand adder.



Proposed 32-bit Brent Kung Adder

REFERENCES:

[1] Koren, Computer Arithmetic Algorithms. Natick, MA, USA: A KPeters, 2002.
[2] David h,k hoe, Chris Martinez and sri jyothsna vundavalli "Design and characterization of parallel prefix adders using FPGAs", Pages.168- 172, march2011 IEEE.
[3] K.Vitoroulis and A.J. Al-Khalili, "performance of parallel prefix adders implemented with FPGA technology," IEEE Northeast Workshop on circuits and systems, pp.498-501, Aug. 2007.
[4] Haridimos t.vergos, Member, IEEE and Giorgos Dimitrakopoulos, Member, IEEE,"On modulo 2n+1 adder design"IEEE Trans on computers, vol.61, no.2, feb 2012
[5] Giorgos Dimitrakopoulos and Dimitris Nikolos, "High-Speed Parallel-Prefix VLSI Ling Adders" IEEE Trans on computers, vol.54, no.2, Feb. 2005.

[6] S.Knowles,"Afamily ofadders," Proc.15th Symp. Comp. Arith.,pp.277-281,June2001.
[7] R.BrentandH.Kung,"Aregularlayoutfor parallel adders, "IEEETrans. Computers, vol.C-31, no.3, pp. 260-264, March1982.
[8] R.E. Brent and M.J. Kung, "Parallel Prefix Computation," J. ACM, vol. 27, no. 4, pages 831- 838, Oct. 1980.
[9] K. Du, P. Varman, and K. Mohanram, "High performance reliable variable latency carry select addition," in Proc. Design, Autom., Test Eur.Conf. Exhib. (DATE '12), Mar. 2012, pp. 1257–1262.
[10] Sudheer Kumar Yezerla, B RajendraNaik, "Design and Estimation of Delay, Power and Area. for parallel prefix adders*", proceedings of 2014 RAECS UIET Panjab University Chandigarh*, 06-08 March, 2014.
[11] Anas Zainal Abidin, Syed Abdul Mutalib Al Junid,Khairul Khaizi Mohd Sharif, Zulkifli Othman, Muhammad AdibHaron, "4-bit Brent Kung Parallel Prefix Adder Simulation Study Using Silvaco EDA Tools",DOI. 10.5013/IJSSST.a.13.3A.07.
[12] Pappu P. Potdukhe, Vishal D. Jaiswal, "Design of high speed carry select adder using Brent kung adder*", IEECOT,International conference, Chennai, India*, 03-05 March 2016.
[13] Kostas Vitoroulis, "Parallel Prefix Adders", Concordia University, 2006
[14] Pakkiraiah. Chakali, madhu Kumar. Patnala "Design of high speed Ladner - Fischer based carry select adder" IJSCE, Volume-3, Issue-1, March 2013.

~Rajini Kumar (16761D6818)

2. Wide Band micro strip patch antenna

The main success of microstrip patch antenna is thus it is meeting the satisfactions of new generation technology. The last few years' study says that the patch antenna structures improving from one year to the next year based on the performance. The main use of patch antenna is when it is incorporated in mobiles for mobile communications to decrease severe radiation. Several shapes are designed in order to reduce the effect of radiation [2-4].

The less use of microstrip patch antenna was because of its narrow band range, less distance propagation and its poor efficiency. To make narrow band to wide band many procedures have been done and are raised in the subject of antenna design. [6].

The main use of the microstrip patch antenna in the present remote correspondence framework was because of its low profile characteristic; size is compactable, consistably configurable, minimal effort, simple to manufacture and coordinate. Patch is the main part of the microstrip patch antenna and ground, substrate are the other parts of it. The patch is printed on the substrate [5].

The main reason to reduce the size of the patch antenna were to improve the bandwidth and it can also be accomplished by creating slots on the both ground and on the patch. The slots are created by taking proper length and width of the slots [1, 7-9]. The main problem that scientists and researchers facing is to design an antenna in the X band range and Ku band range because of its use in satellite and radar communications. For such type of antennas, the band required is wide band, it has high bit rate and distance range is less. So now the challenge is to satisfy the above three properties [9-10].

A rectangular microstrip patch antenna is designed in this reference which has a unique layer and bandwidth is felt short of 20 percent. This antenna has a bandwidth of 1 GHz and it is achieved with a low gain of 1.5dB at the operating frequency [12 In this reference an antenna was proposed which has a high bandwidth and the antenna structure has a circularly rotatable patch structure. The slot enhances the bandwidth. [13].

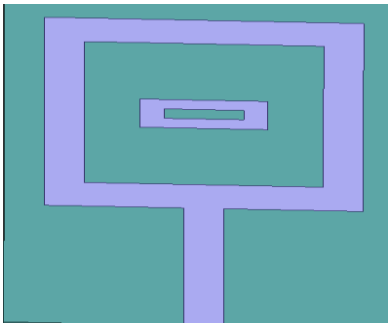
The antenna proposed in this reference has both length and width of 70mm that makes it a giant look like structure. Apart from this all the results are good for this structure, it has a large wide band of bandwidth 2ghz with a magnitude gain of 2dB at its operating frequency [14]. Two slot antennas which are in E-shaped were designed. This antenna has both length and width of 85mm that makes the structure large and less compactable. The results of this antenna are pretty good in gain and bandwidth with the

help of microstrip line and CPW feeding technique. By looking the entire structure, it looks like a fork standardization stub to enlarge the bandwidth [11].

This article mainly focuses on the antenna parameters like return loss and VSWR at two operable frequencies. In this paper three different patch structures are designed with only FR4 substrate material, the three structure designed such a way that only rectangular slots are created on the substrate and the ground is left as plane. The three structures are operable in the range of 8-16 Ghz and their characteristics are known with the help of HFSS.The three different structures are discussed below this section and the substrate thickness is 1.6 in all the three cases and lumped port excitation is given every structure.

ANTENNA STRUCTURES AND DESIGNS:

The geometry of the designed antenna structure 1 has been shown in Fig. 1. The antenna comprises of a rectangular slot on the radiating patch. The rectangle slot is kept inside the main radiating patch. The second antenna structure has a hexagonal slot inside the patch and the two rectangular slots one inside the other is placed adjacent to the main patch and it is shown in Fig. 2. The third design structure which is shown in Fig. 3 is quite similar to that of the previous structure but the main change is that the adjacent patch structure here is a U shaped slot which is rotated. The design process begins with the radiating patch with substrate, ground plane and a feed line. It is printed on a 1.6 mm thick FR4 substrate that contains relative permittivity of 4.4 and relative permeability of 1. The ground is kept plane in all the three structures and the lumped port excitation is given for the three structures.



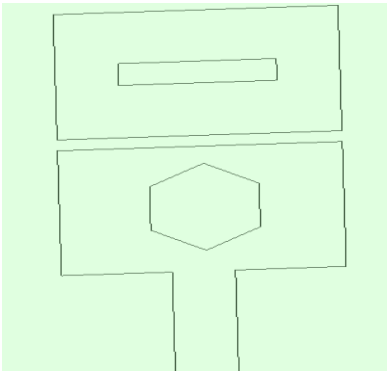


Fig1:Structure of Antenna 1 Top View Fig 2:Structure of Antenna 2 Top View

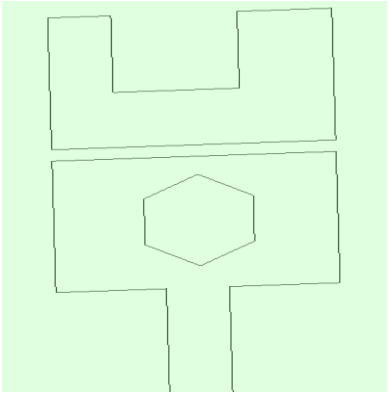


Fig 3:Structure of Antenna 3 Top View

REFERENCES:

[1] M. M. Islam, M. T. Islam, M. R. I. Faruque, W. Hueyshin, "Design of an X-band microstrip patch antenna with Enhanced bandwidth", IEEE 2013

[2] M. T. Islam, M. R. I. Faruque and N. Misran, "Anaylasis of electromagnetic absorption in mobile phones using metamaterials," *Electromagnetics*, vol. 31, no. 3 pp. 215-232,2011.

[3] M. R. I. Faruque, M. T. Islam and N. Misran, "Evaluation of specific absorption rate (SAR) reduction for PIFA antenna using metamaterials," *Frequent*, vol. 64, no. 7-8, pp.144-149,2010.

[4] M. T. Islam, M. R. I. Faruque and N. Misran, "Design analysis of ferrite sheet attachment for SAR reduction in human head," *Progress In Electromagnetics Research*, vol. 98, pp. 191-205,2009.

[5] L. H. Weng, Y. –C. Guo, X. –W. Shi, and X. –Q. Chen. "An overview on defected ground structure." *Progress In Electromagnetics Research B*, vol. 7, pp. 173-189,2008.

[6] K. Kiminami, H. Akimasa, and S. Toshiyuki, "Double-sided printed bow-tie antenna for UWB communications." *IEEE Antennas and Wireless Propagation Letters*, vol. 3, no. 1, pp. 152-153,2004.

[7] T. S. See and Z.N. Chen, "An electromagnetically coupled UWB plate antenna," IEEE Trans. Antennas Propag, vol. 56, no. 5, pp. 1476-1479, 2008.

[8] M. R. I. Faruque, M. T. Islam and N. Misran, "Evaluation of specific absorption rate (SAR) reduction for PIFA antenna using metamaterials," *Frequent*, vol. 64, no. 7-8, pp.144-149,2010.

[9] J. X. Xiao, M. F. Wang, and G. J. Li, "A ring monopole antenna for UWB application," *Microw. Opt. Technol. Lett.*, vol. 52, no. 1, pp. 179- 182,2010.

[10] M. Samsuzzaman, M. T. Islam, and M. R. I. Faruque, "Dual-band multi slot patch antenna for wireless applications, *"Journal of Telecommunications and Information Technology*, vol. 2, pp. 19-23, 2013.

[11] J.-Y. Sze, and K. -L. Wong, "Bandwidth enhancement of a microstrip line-fed printed wide-slot antenna," *IEEE Trans. Antennas Propag.* vol. 49, no. 7, pp. 1020-1024,2001.

~ K.V.N.Kavya(15761A04D9)
CH.J.V.Madhavi (15761A04E6)
K.Vinay Kumar(15761A04F3)
M.Narendra Kumar (16765A0428)

3.Smart Walking Assist

INTRODUCTION:

Identifying a location and tracing the location by choosing specific directions are prominent aspects of any human life. Human visual system is designed in such a way to discriminate the situations or environment that is either safe or risky. With ever increasing diabetic problems as well as the visual impaired by birth are the challenges for human beings to perform daily tasks. Factors like genetics, infection or injury may result in either temporary or blindness. Such a people have a difficulty in navigating to areas where they are not yet acquainted. The problem is serious if the impaired person need to spend in an environment i.e., crowded with people or in a traffic area. They are not able to identify the presence of an object in the surrounding environment. Even if the effected person tries to walk over the footpaths, the presence of vendors, animals and other obstacles cause difficulties. According to a survey by World Health Organization (WHO), nearly 285 million people have visual problem majority of them are suffering with low vision.

With the development of technology, effects have been made to develop such a system which can help the blind people to perform their daily activities without any assistance. Developing an electronic system for visually challenged people is one among the significant research area these days. The system developed should be economical as well as simple in operation. The current work aims at developing a smart stick i.e., capable of eliminating from any hazardous situations like mud pits /water, fire and obstacles in the vicinity of his/her surroundings.

EXISTING WORK:

The fundamental requirements of a visually challenged person were addressed in[1]. It was mentioned that the device developed should be non noisy and capable of detecting the obstacles effectively. The distance between the person and obstacle is calculated by using optical triangulation.

A movable cane embedded on wheel platform was developed in [2].Pair of ultrasonic sensors are utilized for sensing the obstacle in the path of the blind person that automatically moves by rotating the servo motor. The direction of travel is decided by the user who predefines the way of travel.

A navigational system that helps the shopping by a visually challenged person eases was presented in [3].Laser beam is used in the process of determine the distances between the person and the object by means of which the location is tracked accurately.

The experiences of person suffering from visual impairedness were shared and included in developing technology that assists blind person as presented in [4]. All the considerations that were needed for improving the accuracy of navigation by blind people were addressed.

A handset that is capable of guiding for fully as well as partially impaired persons in visualization, was described in [5].Little large in size than a mobile handset, the designed system has proven its accuracy in the process of effective positioning.

A system that supports the needs of blind people in navigating is presented in [6].The systems made use of minimum hardware with less weight and is capable of adapting to training as and when required ultrasonic sensors are used in the process identifying obstacles in multiple direction.

In [7], the vibration of the phone as well as alerting through messages to the impaired persons is used as the precautionary measures in the process of developing a supporting system. In addition to identifying the where about the needy person, live streaming through video is also implemented in the developed system.Wearable ultrasonic An obstacle finder based on ultrasonic sensors was proposed in [8].

This system uses ultrasonic sensor which is attached to the both sides of goggles. This project can detect the vehicles which is present in front of the blind person. A smart stick for the blindwas proposed in [9] that consists of Ultrasonic sensor and Arduino board. When the blind person is near to the obstacle the ultrasonic sensor senses it and the vibrator starts beeping. The limitation of using this system is that it doesn't give any information about the location of visually impaired. It just alerts the person about the presence of obstacle.

In[10] , Object detection stick for visually impaired was presented that inherits the basics of image analysis in the process. This system consists of camera, memory element and the camera is attached to the stick which is capable of taking 15 images per second and the object is detected based on the concept of image processing. The disadvantage of using this system is that it requires a memory element for the storage of images and the system is very costly because here we are using a camera.

REFERENCES:

[1]. Benjamin J. M., Ali N. A., Schepis A.F.,- "*A Laser Cane for the Blind*", Proceedings of the San Diego Biomedical Symposium, Vol. 12, 53-57,1967.

[2]. Johann B., Iwan U.,"*The Guide Cane – A Computerized Travel Aid for the Active Guidance of Blind Pedestrians*", Proceedings of the IEEE International Conference on Robotics and Automation, Albuquerque, NM, 1283-1288,1997.

[3]. Kulyukin V., Gharpure C., and Nicholson J., - Robo- Cart: "*Toward Robot-Assisted Navigation of Grocery Stores by the Visually impaired"*, IEEE/RSJ International Conference on Intelligent Robots and Systems, Edmonton, CA.,2005

[4]. Shinohara, K.- "*Designing assistive technology for blind users*", In proceedings of the 8th International ACM SIGACCESS Conference on Computers and accessibility, ACM, 293-294, 2006.

[5]. Madad A. Shah, Sayed H. Abbas, Shahzad A. Malik, - "*Blind Navigation via a DGPS based Hand-Held Unit*", Australian Journal of Basic and Applied Sciences, 4(6): 1449-1458, 2010.

[6]. Kang. S. J., Ho. Y. K., & Moon. I.H., "*Development of an Intelligent Guide - Stick for the Blind".* Seoul, Korea, IEEE March 2013.

[7]. ShrutiDesai,Mrunali Bichukale,Shraddha Kamte, Archana Borate,A.G.Nadapah, "*Smart Blind Stick for Visually Impaired People with Live Monitoring"*, IRJET,Volume:03 Isuue:09,Sep-2016.

[8]. Akhila. S,,Divyashree. D ,Disha M Rani ,Varshini.S. "*Smart Stick for Blind using Raspberry Pi*", International Journal of Engineering Research & Technology (IJERT),Volume 4 , Issue 22, 2016.

[9]. Anjali J Suresh., Sruthi A., Revathy Prasannan, Malavika Bhasy., Soumya Murali. "*Smart Cane for Blind*", International Research Journal of Engineering and Technology Volume 05 Issue 05. 2018.

[10]. D.Sathya,S.Nithyaroopa,P.Betty,G.Santhoshni,S.Sabharinath, M.J.Ahanaa,"*Smart Walking stick for blind person*", International Journal of Pure and Applied Mathematics Volume:118 No:20.,2018.[10]

~M.Sravani(15761A0427)
M.Durga Bhavani(15761A0425)
K.Madhu(15761A0421)
V.Dileep(15761A0456)

4.Electrocardiogram

Heart is the muscular which pumps blood through blood vessels of circulatory system. To detect heart problems ECG is used. The electrocardiogram is a non-invasive diagnostic test that evaluates your heart's electrical system to access for heart disease. Electrocardiograph is the machine used to produce electrocardiogram. The process of recording the electrical activity of heart over a period of time using electrodes is called electrocardiography.

There are number of conditions that can be detected while checking a pulse. ECG wave patterns verifies also those and also certain changes in wave provides information about specific type of heart disease and affected region in heart.

ECG is safe test that does not cause any health complications. There are no medical conditions associated with an increased risk or adverse side effects from ECG. The complete session takes five minutes of time and no side effects.

An ECG is also required prior to any type of heart surgery, including surgery or pacemaker placement. A pre-operative screening ECG is required prior to any surgical procedure that involves general anesthesia and because heart disease increases the risk of adverse events from general and because this helps your anesthesiologists as they plan your anesthetic medications and surgical monitoring.

ECG have some types which have different usage applications. *Cardiopulmonary exercise test* is used to detect any cardiac or pulmonary diseases. *Stress or treadmill test* is used to detect coronary artery disease and to determine safe levels of exercise following a heart attack or heart surgery. *Holter monitor* is used to monitor the ECG tracing continously for a period of 24hours or longer. *Resting 12-lead EKG* is the standard test for measuring heart's electrical function. *Signal -averaged electrocardiogram* by using this a multiple ECG tracings are obtained over a period of approximately 20 minutes in order to capture abnormal heartbeats which may occur intermittently.

A total of ten electrodes are attached with a sticky, but easy to remove adhesive. One electrode is placed on each arm and leg, and six on the chest. Electrodes are the actual conductive pads attached to body surface. Any pair of electrodes can measure the electric potential difference between two corresponding locations of attachment. The electrical signals generated from the electrodes are processed to obtain the heart's electrical activity from 12 different angles, each of which shows a separate tracing. Interpreting the results of ECG involves *tracing* and *follow-up* process.

Limitations for ECG:

- ECG reveals the heart rate and rhythm only during the few seconds it takes to record the tracing.
- ECG is often normal or nearly normal with many types of heart disease , such as *coronary artery disease.*
- Some times, abnormalities that appear on the ECG turn out to have no medical significance after a thorough evaluation is done.

Numerous diagnoses and findings can be made based upon electrocardiography.

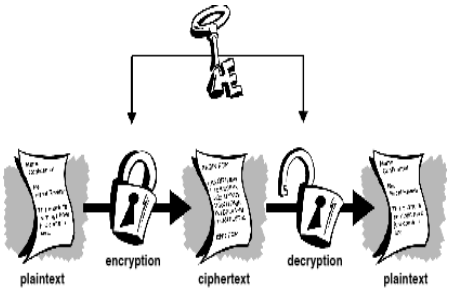
ECG tracing is affected by patient motion. Some rhythmic motions can create the illusion of cardiac arrhythmia. Artifacts are distorted signals caused by a secondary internal or external sources such as muscle movement or interference from an electrical device. Such distortions are to be avoided.

~ Manasa (17761A04E3)

5.Triple Image Encryption

INTRODUCTION:

The image security problem can be solved efficiently and accurately using techniques like Bit-plane shuffling, DNA sequences for image encryption provide confidentiality and authenticity using SHA-256(Secure Hash Algorithm) and XOR of matrices using PWLCM method.



Due to the non-periodicity and affectability to the underlying quality, riotous guide is by all accounts a device that can be utilized for picture encryption. An algorithm for triple image based on chaotic sequences with Deoxyribonucleic acid (DNA) rules and its operations with excellent performance. Firstly, SHA256 hash value of combinational plain images one behind other and 16 bits were taken and are utilized to create introductory estimations of framework parameters of tumultuous frameworks for perplexity and use DNA rules for diffusion process. Then, each 8 bit planes of the three basic images remain knotted built on sequences generated by logistic map. After that each image is segmented into 8 blocks then sequences generated by lts,tss,lss order of these sequences are determined, based on this DNA rules are selected for each block of image. Then, image is shuffled using sine and tent maps. For DNA decoded image bitwise xor operations are done with random image generated by pwlcm. Test results and security examination validate that the calculation has belongings of enormous key space, tall affectability to important, solid opposing to measurable and differential assault.

RELATED WORK:

With advancement of networked multimedia techniques and internet, provides a way

to send image information over various communication channels [1]. To protect that image information from illegal copying and distribution is big challenge today and challenges are increasing day by day from hackers. By using image encryption algorithms, the sender encrypts the plaintext into the cryptograph script. Just the approved beneficiary could unscramble the figure content with the mystery key(s) to acquire the plaintext. With rapid development in technology high data rates can be achieved, but now the problem is to send it in secured manner. This makes to follow the procedure of complex parallel data processing at higher speeds[7,8]. Turbulent frameworks have productive qualities, for example, high affectability to beginning conditions and framework parameters, ergodicity, blending, etc, confusion based picture encryption calculations are recommended increasingly secure and quick encryption techniques which take after wanted cryptographic properties.Tumult based picture encryption calculations can be ordered into three kinds: perplexity, dispersion strategy and aggravating structure. The disarray calculations just scramble the places of the plain-picture pixels.

Histograms of together basic-image and cryptograph-image remain same since pixel values are constant. There are many methods to describe permutation algorithms and can be iterated many times. The diffusion algorithm provides a way to change pixel values of plain image. Recent studies suggest that bit plane decomposition method is one of excellent method in diffusion process which is presented here. So, diffusion procedure is must to make it more secure. For all the picture encryption calculations, the figure picture ought to be shifted extraordinarily from its unique structure. Of this variation container be slow in two ways: NPCR and UACI. NPCR alludes to amount of pixels alteration degree while one-pixel of the basic picture remains altered, and UACI alludes to bound together average changing force that estimates the normal power of contrasts between the plain picture and the figure picture [2,3]. More encryption rounds can attain better encryption consequence, yet more adjusts would devour additional time that had been not utilized in this calculation so as to accomplish tasteful outcomes.

TRIPLE IMAGE ENCRYPTION:

Many picture encryption calculations were proposed dependent on 1D or 2D tumultuous maps/frameworks. The 1D chaotic system have a nature of simplicity in structure and are easy of implementation, in any case, they also have a few imperfections, for example, little key space and powerless security. For improvisation in the security of these encryption algorithms, the higher dimensional systems were used. Be that as it may, the high dimensional frameworks are unpredictable in their structures and

various parameters were utilized which increment in the expense of equipment/programming usage and the calculation multifaceted nature [4,5]. Be that as it may, numerous turmoil based picture encryption calculations are not verify enough, which can be split by means of certain assaults, for example, picked number gratified attack, realized simple content assault and selected basic gratified attack. The new 1D riotous framework was produced after the Logistic, Tent and Sine charts. The new 1D tumultuous framework must bigger confused range and preferred turbulent practices over those seed maps, which makes to utilize these appropriate maps for picture encryption in a superior manner.

Any Encryption calculation to be effective, the calculation should comprise of both disarray and dispersion. Here comes dispersion impact and couple of realities as pursues, for example, shading picture encryption dependent on DNA arrangement task, they changed three Hamming separations of the basic picture into decimal numbers. The picture encryption dependent on DNA subsequence activity and confused framework. Couple pictures encryption calculation uncovers the actualities. To recover the safety of the cryptosystem utilized the riotous framework to irritate the picture pixel locations and pixel esteems, besides after that achieved DNA trainings as indicated by quaternary cipher rubrics.

REFERENCES

1. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci 273:329–351
2. Chai, X., 2015. An image encryption algorithm based on bit level Brownian motion and new chaotic systems. Multimedia Tools and Applications, pp.1-17.
3. Zhou, S., Wang, B., Zheng, X. and Zhou, C., 2016. An Image Encryption Scheme Based on DNA Computing and Cellular Automata. Discrete Dynamics in Nature and Society, 2016.
4. Liu, H. and Wang, X., 2013. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. Journal of Systems and Software, 86(3), pp.826-834.
5. Dixit, A., Dhruve, P. and Bhagwan, D., 2012. Image encryption using permutation And rotational xor technique. Natarajan Meghanathan, et al.(Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT, 6, pp.01-09.

~M.Krishna Priyanka (15761A0488)
A.Ramya Sree(15761A0477)


BLOCK-IV
ELECTRONICS & COMMUNICATION ENGG.
ELECTRONICS & INSTRUMENTATION ENGG.