KIET IJCE

KIET International Journal of Communications & Electronics

VOLUME 3, SECOND ISSUE, JULY-OCT 2014, ISSN:2320-8996

Department of Electronics and Communication Engineering
KIET GROUP OF INSTITUTIONS
(An Integrated Campus approved by AICTE)
Accredited by NAACeith Grade 'A', NBA Accredited and ISO 9001-2000
13-Km Stone, Ghaziabad-Meerut Road,
Ghaziabad-201206, UP, INDIA
Ph: 0120-2675314/315, Tele- 01232-227978
www.kiet.edu

President

Dr. Sraban Mukherjee
Director
KIET Group of Institutions
(NAAC 'A' Grade, NBA Accredited and ISO 9001-2000)
13-Km Stone, Ghaziabad-Meerut Road,
Ghaziabad-201206, UP, INDIA

Vice President

Dr. Manoj Goel
CAO
KIET Group of Institutions
(NAAC 'A' Grade, NBA Accredited and ISO 9001-2000)
13-Km Stone, Ghaziabad-Meerut Road,
Ghaziabad-201206, UP, INDIA

Dr. Gajendra Singh
Additional Director
KIET Group of Institutions
(NAAC 'A' Grade, NBA Accredited and ISO 9001-2000)
13-Km Stone, Ghaziabad-Meerut Road,
Ghaziabad-201206, UP, INDIA

Editor in Chief

Dr. Sanjay Sharma
Professor & Head, ECE Department
KIET Group of Institutions
(NAAC 'A' Grade, NBA Accredited and ISO 9001-2000)
13-Km Stone, Ghaziabad-Meerut Road,
Ghaziabad-201206, UP, INDIA
Email ID: - drsanjaysharma15@gmail.com

Editors

Dr. Vibhav Kumar Sachan,
Additional HoD, ECE Dept., KIET, GZB, U.P.
Ms. Shipra Srivastava

Editorial

Speech is one of the natural forms of communication. Different speech sounds can be characterized by set of spectral and temporal properties which depend on the speech features such as speech waveform or speech spectrum. The speech recognition system contains two main tasks- Feature Extraction and Feature Matching. Feature extraction is the process that extracts a small amount of data from the voice signal that can later be used to represent each spoken word. Feature matching involves the actual procedure to identify the actual spoken words by comparing extracted features from set of known database.

A wireless ad hoc sensor network (WSN) is made up of a number of geographically spread apart sensors each with a reasonable amount of signal processing and data networking ability coupled with wireless communication. One of the major challenges wireless sensor networks face today is security. Denial of service (DoS) attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. This journal explores resource depletion attack in a cooperative manner and increasing traffic on the routing layer protocol. The ease of carrying out a NONACK (Noose Noose attack) and the difficulty in its detection makes all examined protocols very susceptible to it. The worst case scenarios can see an upsurge in the network-wide usage by a factor of O (N^2), N being the number of network nodes.

CMOS technology presents some unsolved problems after shrinking certain limits. Thus for solve these problems new devices developed in place of CMOS in nanoscale era. These problems point to the need for a new kind of fundamental device and architecture, such as quantum-dot cellular automata (QCA).

We take this opportunity to thank all those contributors, reviewers in making this issue a memorable one. Suggestions and feedback from our readers are welcome for the overall improvement of quality of the Journal.

Preface

Dear Researchers,

We take this opportunity to welcome you all to the second issue of International Journal of Communications & Electronics (KIET - IJCE). This journal will provide a forum for in depth and substantial discussions on the theory, design and implementation of the emerging technologies in Communications, Networking, Microwave and Electronics techniques, thus providing solutions and strategies for business resilience.

It gives us an immense pleasure to have an amalgam of researchers from the fields of Communication Engineering, Electronics, and related technologies. The purpose of the Journal is to provide a platform to foster interdisciplinary communication among the delegates and to support the sharing process of diverse fields in various concepts and principles related to these domains.

Our appreciation also goes to entire team whose dedication and timeless efforts have gone for number of days for the second issue of the Journal.

Editors

Message

I am delighted to note that the Department of Electronics and Communication Engineering, KIET Group of Institutions, Ghaziabad is introducing Volume No 2, Issue No. 2 of International Journal of Communications and Electronics (KIET - IJCE).

I appreciate the efforts on the part of the Editorial Committee in bringing out an issue on Communications, Networking, Microwave and Electronics techniques.

I understand that the papers contributed for publication in the Volume No 2, Issue No. 2 are on almost all the current aspects of Communication Systems, Electronics systems, Microwave Engineering, Signal Processing & Applications, Networking Technologies and several others.

I have great pleasure in congratulating the Editors of this issue of KIET - IJCE for their untiring efforts in bringing out this Volume No 2, Issue No. 2 of KIET-IJCE which will be a valued treasure for all who pursue research in Communications, Networking, Microwave and Electronics Engineering areas.

Let me close with warmest regards.

Dr. Sraban Mukherjee
President
KIET – IJCE

Message

It gives me immense pleasure in writing this foreword for the Volume No 2, Issue No.2 of the KIET International Journal on Communications and Electronics (KIET - IJCE). This journal is targeted towards researchers, professionals, educators and students to share innovative ideas, issues, recent trends and future directions in the fields of Electronics and Communication Engineering.

The Volume No 2, Issue No. 2 of the journal KIET-IJCE includes papers on the theory, design and implementation of the emerging technologies in the field of Communications, Networking, Microwave and Electronics techniques. Furthermore, it will enable the researchers in various domains to foster the exchange of concept, protypes, research ideas and the results of research work which could contribute to the academic arena and also befit business and industrial community.

Dr. Sanjay Sharma
Editor – in - chief
KIET - IJCE

SECOND VOLUME
SECOND ISSUE
(JULY-OCT 2014)

KIET IJCE

KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

A Review on 3D Face Recognition Techniques

Prof. Yagnesh J. Parmar[1], Prof. Kunal M. Pattani[2]
Department of Electronics & Communication Engineering, C. U. Shah collage of engineering & technology, Wadhwan, Gujarat, India
yagu_ecengineer@yahoo.com[1], kunalpattani@gmail.com[2]

Abstract—**In this paper, the exploration of new face recognition technology that is 3D face recognition is being analyzed. Face Recognition is widely used for security at many places like airport, organizations, many devices etc. The challenges faced in 2D face recognition technology is been solved through various approaches mentioned in the paper. The various techniques are adapted for 3D face recognition like Principal Component Analysis , Independent Component Analysis, Linear Discriminate Analysis but we focus on Linear Discriminate Analysis. The various implementation approaches widely accepted is been discussed. Each process in the face recognition consists of sub-process and the sub-process is categorized into registration, representation, extraction of discriminative features.**

Keywords—Face recognition; range image; PCA; LDA; ICA; Eigen faces.

I. INTRODUCTION

Now a days with the network world, the way for crime is become easier than before. Because of this reason, network security has become one of the biggest concerns facing today's IT departments. .We heard a lot about hackers way to steal any password or pin code, crimes of ID cards or credit cards fraud or security breaches in any important building and then reach any information or important data from any organization or company. These problems allow us to know the need of strong technology to secure our important data. This technology is based on a technique called "biometrics". Biometric is a form of bioinformatics that uses biological properties to identify people. Since biometric systems identify a person by biological characteristics, they are difficult to fake. Examples of biometrics are iris scanning, signature authentication, voice recognition and hand geometry. Face Recognition is the process to identify the input test face from the stored dataset. Face Recognition Technology (FRT) is used in several disciplines such as image processing, pattern recognition, computer vision etc. in which research is been continuously carried out. More recently face recognition as a "biometric technology (whereby the face is physiological trait that uniquely identifies an individual) has become a hot topic of modern day research as a result of the growing pressure to exploit faces as a means of identification from both the commercial and law enforcement. New databases have been created and evaluations of recognition techniques using these databases have been carried out. Now, the face recognition has become one of the most active applications of pattern recognition, image analysis and understanding.Automated face recognition technologies are also in use in both the civilian and Law enforcement areas.Face Recognition fall into two categories: verification and identification. Face verification is a 1:1 match that matches a face against the template face images whose identity is to be claimed. Face identification is 1:N problem that compares a query face image against all image templates in face database to determine the identity of the query face. During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson [2], worked on using computers to recognize human faces at Stanford institute. Bledsoe designed and implemented a semi-automatic system. Some face coordinates were selected by a human operator, and then computers used this information for recognition. He described most of the problems that even 50 years later Face Recognition still suffers - variations in illumination, head rotation, facial expression, and aging. Researches on this matter still continue, trying to measure subjective face features as ear size or between-eye distance. For instance, this approach was used in Bell Laboratories by A. Jay Goldstein, Leon D. Harmon and Ann B. Lesk [3] in which how well can human faces be identified by humans and by computers, using subjectively judged "feature" descriptions like long ears, wide-set eyes. Although the first fully functional implementation of an automated faces recognition system was not produced until Kanade"s paper [4] in 1977. They described a vector, containing 21 subjective features like ear protrusion, eyebrow weight or nose length, as the basis to recognize faces using pattern classification techniques. In the last five years, a rapid increase for the need to design 3D face recognition algorithms has taken place both in academy and industry. However, it is clearly visible that the 3D face recognition technology is at the beginning steps. The motivation to use 3D technology was to overcome the disadvantages of 2D face recognition systems that arise especially from significant pose, expression and illumination differences. However, with the exception of few recent works, most of the 3D systems generally study controlled frontal face recognition. With the construction of bigger 3D face databases that contain enough samples for different illumination, pose, and expression variations, it is expected to develop more realistic 3D face recognition.

II. CHALLENGES IN FRT

There are two major challenges faced during the testing, those are illumination problem and pose variation problem. Both these problems are serious and cause the degradation of

the existing system. These problems can be formulated and a common approach could be followed by sequencing the operations face detection, face normalization and inquire database.

A. Illumination Problem

Same image may appear differently due to illumination condition. If the illumination induced is larger than the difference between the individuals, system may not be able to recognize the input image. It has been suggested that one can reduce variation by discarding the most important eigenface. And it is verified in [5] that discarding the first few eigenfaces seems to work reasonably well. Many of the methods were suggested by researchers which ultimately led to the result that the methods were illumination-invariant and the measure of the same object changes when illumination changes. An illumination subspace can be constructed but one drawback of this method is that many of the faces of one person are needed to construct the subspace. Methods have been developed to solve the illumination problem the approaches have been divided into four categories: First is heuristic methods including and discarding the leading principal components. Second, image comparison methods where various image representations and distance measures are applied. In class-based methods where multiple images of one face under a fixed pose but different lighting conditions are available. Finally in model-based approaches 3D models are employed.

B. Pose Problem

Researchers have proposed various methods to handle the rotation problem. Basically they can be divided into three classes: a). multiple images based methods: when multiple images per person are available. This method is based on illumination cone to deal with illumination variation. For variations due to rotation, it needs to completely resolve the GBR (generalized-bas-relief) ambiguity when reconstructing 3D surface. b). hybrid methods: when multiple training images are available during training, but only one database image per person is available during recognition. Numerous algorithms of the second type have been proposed and are by far the most popular ones. Possible reasons for this are: i) It is probably the most successful and practical method up to now, ii) It utilizes prior class information., and c).single image/shape based methods when no training is carried out. In these methods, face shape is usually represented either by a polygonal model or a mesh model which simulates issue.

III. Depth Based Approach

It is very popular to convert 2.5D facial data to a depth image, also called the range image. Each pixel in the depth image represents the distance of the corresponding 3D facial point to the camera. Although some sensors are capable of producing range images directly, point cloud data acquired from sensors is usually converted to yield depth images. During the conversion, some information may be lost. Most importantly, two sources of information loss should be mentioned: Firstly In the surface areas whose normal are almost perpendicular to the camera view, such as the lower nose regions, a significant portion of the depth measurements is generally under-represented in the depth images, and Secondly, 8-bit standard gray-level quantization may lose accuracy information. Another important concern in depth image construction is the conversion of irregularly sampled 3D points to a regular (x, y) grid. To accomplish this task, interpolation methods are generally used.

A. Principal Component Analysis (PCA)

PCA also known as Karhunen-Loeve method is one of the popular methods for feature selection and dimension reduction. The recognition method, known as eigenface method defines a feature space which reduces the dimensionality of the original data space. This reduced data space is used for recognition. But poor discriminating power within the class and large computation are the well known common problems in PCA method. This limitation is overcome by Linear Discriminant Analysis (LDA). LDA is the most dominant algorithms for feature selection in appearance based methods [9]. But many LDA based face recognition system first used PCA to reduce dimensions and then LDA is used to maximize the discriminating power of feature selection. The performances of appearance based statistical methods such as PCA, LDA and ICA are tested and compared for the recognition of colored faces images in [11]. PCA is better than LDA and ICA under different illumination variations but LDA is better than ICA. LDA is more sensitive than PCA and ICA on partial occlusions, but PCA is less sensitive to partial occlusions compared to LDA and ICA. PCA is used as a dimension reduction technique in [12] and for modeling expression deformations in [13].A recursive algorithm for calculating the discriminant features of PCA-LDA procedure is introduced in [14]. This method concentrates on challenging issue of computing discriminating vectors from an incrementally arriving high dimensional data stream without computing the corresponding covariance matrix. The proposed incremental PCA-LDA algorithm is very efficient in memory usage and it is very efficient in the calculation of first basis vectors. This algorithm gives an acceptable face recognition success rate in comparison with very famous face recognition algorithms such as PCA and LDA. The main idea is to decorrelate data in order to highlight differences and similarities by finding the principal directions (i.e. the eigenvectors) of the covariance matrix of a multidimensional data. The steps performed in PCA are: First step includes training phase using the Training Set, in order to generalize the ability of our system and generate eigenvectors. Then we compute the mean image of the training data. Then each Training image is mean subtracted. Then the covariance matrix (C) of the mean-subtracted training data is then computed (T) denotes the matrix transposition operation. The next step consists in finding the eigenvectors $en$and the eigenvalues λn of C. A part of the great efficiency of the PCA algorithm is to take only the "best" eigenvectors in order to generate the subspace ("Face Space") where the gallery images will be projected onto, leading to a reduction of dimensionality. Eigen values are sorted in decreasing order (a higher eigenvalue captures a higher variance, hence more information).The mean image of the Gallery Set is computed. Each mean-subtracted gallery image is then projected onto the "Face Space" spanned by the eigenvectors deriving from the

Training Set. This step leads to a simple dot product. Scalars ωk are called "weights" and represent the contribution of each eigenvector for the input image. Thus, for each gallery image, we have a "Weights Vector". The "Weights Matrix" is then generated and stored in the database and will be used during the recognition step we focused on. The Recognition takes place in several steps: The dot product is the first basic operation that must be done during the recognition step. A normalized probe image is projected onto the "Face Space", in order to obtain a vector. The second step is the Distance Measure: Once the incoming probe image has been projected onto the Face Space, we have to see whether it is a known face or not. To proceed, we compute the Squared Euclidean Distance (SED) between the weights from the probe image and the Weights Matrix of the entire Face Space: Finally the minimum Euclidean distance is calculated. Assume the ID of the probe image is the l (from 1 to P) and k is the index corresponding to the minimum SED, a subject is considered as a genuine if l=k, otherwise he is considered as an impostor. The performance of recognition while using PCA as well as LDA for dimensionality reduction seems to be equal in terms of accuracy. But it was observed that LDA requires very long time for processing more number of multiple face images even for small databases.

B. *Independent Component Analysis (ICA)*

In [14], While PCA decorrelates the input data using second-order statistics and thereby generates compressed data with minimum mean-squared reprojection error, ICA minimizes both second-order and higher-order dependencies in the input. It is intimately related to the blind source separation (BSS) problem, where the goal is to decompose an observed signal into a linear combination of unknown independent signals. Let s be the vector of unknown source signals and x be the vector of observed mixtures. If A is the unknown mixing matrix, then the mixing model is written as x = As It is assumed that the source signals are independent of each other and the mixing matrix A is invertible. Based on these assumptions and the observed mixtures, ICA algorithms try to find the mixing matrix A or the separating matrix W such that u =Wx =WAs is an estimation of the independent source signals ICA can be viewed as a generalization of PCA. As previously discussed, PCA decorrelates the training data so that the sample covariance of the training data is zero. Whiteness is a stronger constraint that requires both decorrelation and unit variance. The whitening transform can be determined as D-1/2RT where D is the diagonal matrix of the eigenvalues and R is the matrix of orthogonal eigenvectors of the sample covariance matrix. Applying whitening to observed mixtures, however, results in the source signal only up to an orthogonal transformation. ICA goes one step further so that it transforms the whitened data into a set of statistically independent signals. Signals are statistically independent when the probability density function is equivalent to say that the vectors u is uniformly distributed.Unfortunately, there may not be any matrix W that fully satisfies the independence condition, and there is no closed form expression to find W. Instead, there are several algorithms that iteratively approximate W so as to indirectly maximize independence. Since it is difficult to maximize the independence condition above directly, all common ICA algorithms recast the problem to iteratively optimize a smooth function whose global optima occurs when the output vectors u are independent.

C. *Linear Discriminant Analysis (LDA)*

This approach is also known as fisher-surface approach. In LDA we find the linear transformations such that feature cluster are most separable after transformation. We apply PCA and LDA to surface representations of 3D face models, producing a subspace projection matrix, taking advantage of „within-class" information, minimizing variation between multiple face models of the same person, yet maintaining high class separation. To accomplish this we use a training set containing several examples of each subject, describing facial structure variance (due to influences such as facial expression), from one model to another. From the training set we compute three scatter matrices, representing the within-class (SW), between-class (SB) and total (ST) distribution from the average surface and classes" averages. The training set is partitioned into c classes, such that all surface vectors in a single class are of the same person and no person is present in multiple classes. Calculating eigenvectors of the matrix, and taking the top 250 (number of surfaces minus number of classes) principal components, we produce a projection matrix. This is then used to reduce dimensionality of the within-class and between-class scatter matrices (ensuring they are non-singular) before computing the top c-1 eigenvectors of the reduced scatter matrix ratio. Finally, the matrix Uff is calculated, such that it projects a face surface vector into a reduced space of c-1 dimensions, in which the ratio of between-class scatter to within class scatter is maximized for all c classes. Like the eigenface system, components of the projection matrix Uff can be viewed as images, as shown in Figure. 4 for the depth map surface space. Once surface space has been defined, we project a facial surface into reduced surface space by a simple matrix multiplication. The vector is taken as a „face key" representing the facial structure in the reduced dimensionality space. Face-Keys are compared using either Euclidean or cosine distance measures. An acceptance (facial surfaces match) or rejection (surfaces do not match) is determined by applying a threshold to the distance calculated. Any comparison producing a distance value below the threshold is considered an acceptance.

IV. FACE RECOGNITION TECHNOLOGY

A. *Definition*

As we all know that almost the security system in the airports, huge hotel and especially in the police led depend on the use of advanced protection system that based on the computer programs. Theses program verifying people present and also thieves. This system is based database for pictures of people criminals, thieves and others with picture captured by a surveillance camera. So a facial recognition system is a computer application for automatically identifying a person digital image that its source is already sorted in the database. Actually, it is works by comparing the selected facial features from the image and a facial database.

B. Face Measure

Every human face has many distinctive features are in a various meandering on the face. The program is based on these parameters nodal points. Each face has approximately 80 nodal points. Almost facial recognition programs analyze the relative position, size, and/or shape of the eyes, nose, cheek boons and jaw. The most famous features of the face measured by a program are:

1. The distance between the eyes.
2. The depth of the eye.
3. Nasal breadth.
4. The form of the cheek boon.
5. Along the jaw line.

The parameters measured by the program and then translated into digital codes called the fingerprint and face print used to represent the face in the database.

C. Face Recognition Types

2D System In the past [4], facial recognition programs depended on two dimension (2D) picture to compare it with the image sorted in the data base, but these programs did not succeed only if the person is looking just to the camera. Of course anyone suspect will be warned that he/she will see a camera in place, and here lies the problem where this fails by depending on the 2D system. Beside, the additional changes in the environment surrounding the person, such as light will produce images the computer cannot have in the corresponding memory, also the changes in the same person can cause a system failure in face recognition [5, 6].

3D System Modern system for face recognition based on the pattern of three-dimensional (3D) [8], where the special cameras will captured images of three-dimensional views of the suspected person, and using the special main features of each face that are not changed significantly with time , such as eye hole, the distance between the eyes, nose shape and others mentioned above. These features are a source of information for a facial recognition system as the changes in the lighting or surrounding environmental conditions do not affect these measurements, for example: can operate these systems in any lighting conditions even if the place was dark and even if the person is not in the face of camera.

D. 3D Face Recognition

How 3D Procedure Work: The use of depth and focus of the face that does not affect the change in lighting is known as three-dimensional face recognition system. The software system that relay on three-dimensional technique with a series of steps to eventually be able to perform a face recognition procedure. We can divide the whole process by the following steps. Steps involve in the face recognition system are: (fig 1)

Fig. 1 the steps of 3D face recognition system.

1) Detection: Capture a digital image by a two dimensional digital camera or even using a video camera.

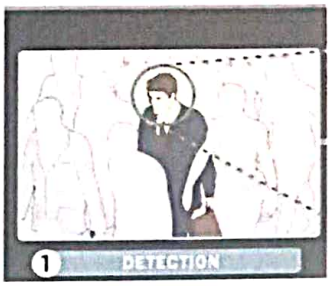


Fig. 1 Detection

2) Alignment: After capturing the image, the system will determine a head position, size and its direction.

Fig. 2 Alignment

3) Measurement: The software (specific program) will calculate the curves and meanders on the face to an accuracy of part OS the millimeter. Then the program ready to convert that information to establish a face model or pattern.

Fig. 3 Measurement

4) Representation: In this step, the system will translate the model and form a specific code. The code for each model is unique and consists of a set of numbers.

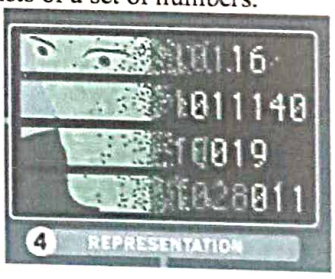


Fig. 4 Representation

5) Matching: In the case that the picture is threedimensional and corresponding to the three- dimensional images that stored in the database, the comparisons between the images are immediately. But the challenge facing these systems is that most of the images stored in database are in two-dimensional.

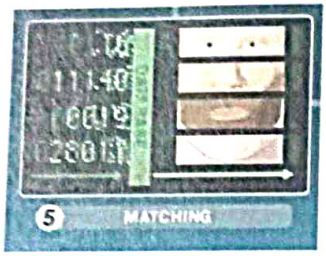


Fig. 5 Matching

The development of a new technology support the use of three different points to get to know any face sorted in database. Some of these points are outside of the eyes, inside the eyes and the tip of the nose. The conduct of the system will carry out these measurements on the dimensions between these points of three-dimensional picture and begin to be converted to two-dimensional images through the application of complex mathematical algorithms. After the conversion process, of this part, the system begins to work of comparison.

6) Verification or Identification: In the step of recognition, the program will compared the images and match them with pictures of the database sorted by the system in the Previous step. But if the goal is verify the result of the previous step, the system compares the image with all images in the database and then matching results are displayed in percentages [3].

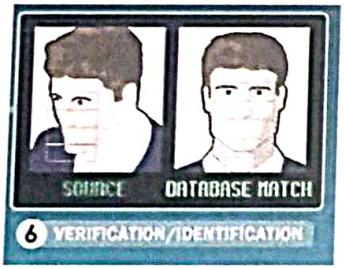


Fig. 6 Verification or Identification

REFERENCES

[1] R. Chellappa, C.L. Wilson, and Sirohey, "Human and Machine Recognition of Faces, A survey," Proc. of the IEEE, Vol. 83, pp. 705-740, 1995.

[2] "Face Recognition Algorithms" Proyecto Fin de Carrera June 16, 2010I on Marqu´es

[3] A. Jay Goldstein, Leon D. Harmon, Ann B. Lesk , "Man Machine Interaction in Human Face Identification", Proceedings of IEEE, USAF, AFIT/GREENG/87D-35; "Neural Networks Primer, Part I", Maureen Caudill.

[4] Jeffrey F. Cohn, Adena J. Zlochower, James Lien, and Takeo Kanade , "Automated face recognition"

[5] Belhumeur, P.N.; Hespanha, J.P.; Kriegman, D.J., "Eigenfaces vs. Fisher faces: recognition using class specific linear projection" Pattern Analysis and Machine Intelligence, IEEE Transactions on , Volume: 19 Issue: 7 , Jul 1997 Page(s): 711 -720

[6] Boulbaba Ben Amor1, Karima Ouji1, Mohsen Ardabilian1, Liming Chen , "3D Face recognition BY ICP-based shape matching" LIRIS Lab, Lyon Research Center for Images and Intelligent Information Systems, UMR 5205 CNRS Centrale Lyon, France.

[7] G. Gordon, "Face Recognition from Depth Maps and Surface Curvature", in Proc. of SPIE, Geometric Methods in Computer Vision, San Diego, July 1991. Vol. 1570.

[8] Beumier, C. and M. Acheroy, "Face verification from 3D and grey level cues", Pattern Recognition Letters, Vol. 22, pp. 1321-1329, 2001.

[9] Beumier, C. and M. Acheroy, "Automatic 3D Face Authentication", Image and Vision Computing, Vol. 18, No. 4, pp. 315-321, 2000.

[10] Zhang, L., A. Razdan, G. Farin, J. Femiani, M. Bae, and C. Lockwood, "3D face authentication and recognition based on bilateral symmetry analysis", Visual Comput (22), p. 4355, 2006.

[11] Feng, S., H. Krim, I. Gu, and M. Viberg, "3D Face Recognition using Affine Integral Invariants", Proc. of. ICASSP, pp. 189-192, 2006.

[12] Tanaka, H., M. Ikeda, and H. Chiaki, "Curvature-based face surface recognition using spherical correlation principal directions for curved object recognition", Third International Conference on Automated Face and Gesture Recognition, pp. 372- 377, 1998.

[13] Turk, M. and A. Pentland, "Eigenfaces for recognition", Journal of Cognitive Neurosciences, Vol. 3, No. 1, pp. 71-86, 1991.

[14] Hyvarinen, A. and E. Oja, "Independent Component Analysis: Algorithms and Applications", Neural Networks, Vol. 13, No. 4-5, pp. 411-430, 2000.

[15] Tanaka, H., M. Ikeda, and H. Chiaki, "Curvature-based face surface recognition using spherical correlation principal directions for curved object recognition", Third International Conference on Automated Face and Gesture Recognition, pp. 372-377, 1998.

[16] Gordon, G., "Face Recognition Based on Depth and Curvature Features", Proc. Of the IEEE Computer Society Conf. on Computer Vision and Pattern Recognition, pp. 108-110, 1992.

[17] Bronstein, A., M. Bronstein, and R. Kimmel, "Three-dimensional face recognition", International Journal of Computer Vision, Vol. 64, No. 1, pp. 5-30, 2005.

[18] C. Nastar and M. Mitschke, "Real time face recognition using feature combination," in Third IEEE International Conference on Automatic Face and Gesture Recognition. Nara, Japan, 1998, pp. 312-317.

[19] S. Gong, S. J. McKenna, and A. Psarrou., Dynamic Vision: From Images to Face Recognition: Imperial College Press (World Scientific Publishing Company),58A Survey of Face Recognition Techniques 2000.

[20] T. Jebara, "3D Pose Estimation and Normalization for Face Recognition," Center for Intelligent Machines, McGill University, Undergraduate Thesis May, 1996.

[21] D. Blackburn, J. Bone, and P. J. Phillips, "Face recognition vendor test 2000," Defense Advanced Research Projects Agency, Arlington, VA, Technical report A269514, February 16, 2001.

KIET KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

A Review on Speech Feature Extraction and Speech Feature Matching Technique

Mr. Mahesh Kumar Patil[1], Prof. Dr. (Mrs.) L.S. Admuthe[2], Mr. Prashant P Zirmite[3], Prof. Mr. N.B. Kapase[4]
Assistant Professor, Electronics Engineering, Textile & Engineering Institute, Ichalkaranji

Abstract- **Speech is one of the natural forms of communication. Different speech sounds can be characterized by set of spectral and temporal properties which depend on the speech features such as speech waveform or speech spectrum. The speech recognition system contains two main tasks- Feature Extraction and Feature Matching. Feature extraction is the process that extracts a small amount of data from the voice signal that can later be used to represent each spoken word. Feature matching involves the actual procedure to identify the actual spoken words by comparing extracted features from set of known database.**

Keywords- **MFCC, LPC, HMM, DTW, Modeling, Testing.**

I. INTRODUCTION

Humans are fairly good at identifying speakers based on their voices alone. The large amount of work in the field of speaker recognition over the previous 30 years has been predicated on the belief that automated systems ought to be able to do as well, or even better, than humans. Yet we still lack a solid understanding of those characteristics of speech that index an utterance as originating in one speaker rather than another.

The general area of speaker recognition encompasses two fundamental tasks: speaker identification and speaker verification. Speaker identification is the task of assigning an unknown voice to one of the speakers known by the system: it is assumed that the voice must come from a fixed set of speakers. Thus, the system must solve a n-class classification problem and the task is often referred to as closed-set identification. On the other hand, speaker verification refers to the case of open-set identification: it is generally assumed that the unknown voice may come from an impostor. Regardless of the specific task at hand, it is common practice to adopt a probabilistic approach that predicts the likelihood that a given speech sample belongs to a given speaker. The base system for speaker recognition is usually composed of a speech parameterization module and a statistical modeling module which are responsible for the production of a machine readable parameterization of the speech samples and the computation of a statistical model from the parameters. The main difference between speaker identification and speaker verification is that in the first case the system provides one model for each speaker, while, in the second case, the system provides a total of two models: one for the hypothesized speaker and one representing the hypothesis that the speech sample comes from some other speaker—the background model.

II. SPEECH RECOGNITION TECHNIQUES

The goal of speech recognition is for a machine to be able to "hear," understand," and "act upon" spoken information. The earliest speech recognition systems were first attempted in the early 1950s at Bell Laboratories. Davis, Biddulph and Balashek developed an isolated digit recognition system for a single speaker. The speaker recognition system may be viewed as working in a four stages.

A. Analysis
B. Feature extraction
C. Modeling
D. Testing/Matching techniques

A. Speech analysis

In speech analysis technique Speech data contains different types of information that shows a speaker identity. This includes speaker specific information due to vocal tract, excitation source and behavior feature. The physical structure and dimension of vocal tract as well as excitation source are unique for each speaker. The speech analysis deals with stages with suitable frame size for segmenting speech signal for further analysis and extracting [2]. The speech analysis is done with following three techniques.

1) Segmentation Analysis: In this case, speech is analyzed using the frame size and shift in the range of 10-30 ms to extract speaker information. Studies have been made in using segmented analysis to extract vocal tract information of speaker recognition.

2)Sub-segmental Analysis: Speech analyzed using

the frame size and shift in range 3-5 ms is known as Sub segmental analysis. This technique is used mainly to analyze and extract the characteristic of the excitation state. The excitation source information is relatively fast varying compared to vocal tract information, so small frame size and shift are required to best capture the speaker-specific information [3].

3) Supra-segmental Analysis: In this case, speech is analyzed by using the frame size and shift of 100-300 ms to extract speaker information mainly due to behavioral tract and speech is analyzed using the frame size.

This technique is used mainly to analyze and characteristic due to behavior character of the Speaker. These include word duration, intonation, speaker rate, accent etc.

B. Feature extraction techniques

Feature Extraction is the most important part of speech recognition since it plays an important role to separate one speech from other. The utterance can be extracted from a wide range of feature extraction techniques proposed and successfully exploited for speech recognition task. But extracted feature should meet some criteria while dealing with the speech signal such as:

i. Easy to measure extracted speech features
ii. It should not be susceptible to mimicry
iii. It should show little fluctuation from one speaking environment to another
iv. It should be stable over time
v. It should occur frequently and naturally in speech

The most widely used feature extraction techniques are explained below.

1) Linear Predictive Coding (LPC):

One of the most powerful signal analysis techniques is the method of linear prediction. LPC [4] of speech has become the predominant technique for estimating the basic parameters of speech. It provides both an accurate estimate of the speech parameters and it is also an efficient computational model of speech. The basic idea behind LPC is that a speech sample can be approximated as a linear combination of past speech samples. Through minimizing the sum of squared differences (over a finite interval) between the actual speech samples and predicted values, a unique set of parameters or predictor coefficients can be determined. These coefficients form the basis for LPC of speech. The predictor coefficients are therefore transformed to a more robust set of parameters known as cepstral coefficients. The figure1 shows the steps involved in LPC feature extraction.

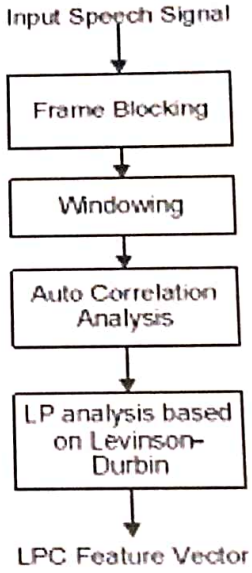


Fig 1. Steps involved in LPC Feature Extraction

2) Mel Frequency Cepstral Coefficients (MFCC) :

The following figure 2 shows the steps involved in MFCC feature extraction. The MFCC [4] is the most evident example of a feature set that is extensively used in speech recognition. As the frequency bands are positioned logarithmically in MFCC it approximates the human system response more closely than any other system. Technique of computing MFCC is based on the short-term analysis, and thus from each frame a MFCC vector is computed.

In order to extract the coefficients the speech sample is taken as the input and hamming window is applied to minimize the discontinuities of a signal. Then DFT will be used to generate the Mel filter bank. According to Mel frequency warping, the width of the triangular filters varies and so the log total energy in a critical band around the center frequency is included. After warping the numbers of coefficients are obtained. Finally the Inverse Discrete

Fourier Transformer is used for the cepstral coefficients calculation.

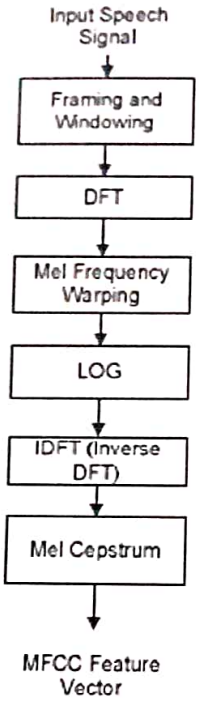


Fig. 2 Steps involved in MFCC Feature Extraction

It transforms the log of the quefrench domain coefficients to the frequency domain where N is the length of the DFT. MFCC can be computed by using the formula (1).

$$Mel(f) = 2595 * \log_{10}(1 + \frac{f}{700}) \quad (1)$$

C. Modeling technique

The objective of modeling technique is to generate speaker models using speaker specific feature vector. The speaker modeling technique divided into two classification speaker recognition and speaker identification. The speaker identification technique automatically identifies who is speaking on basis of individual information integrated in speech signal. The system can recognize the speaker, which has been trained with a number of speakers. Speaker recognition can also be dividing into two methods, text- dependent and text independent methods. In text dependent method the speaker say key words or sentences having the same text for both training and recognition trials. Whereas text independent does not rely on a specific texts being spoken [7]. Following are the modeling which can be used in speech recognition process:

1) The acoustic-phonetic approach

This method is indeed viable and has been studied in great depth for more than 40 years. This approach is based upon theory of acoustic phonetics and postulates. The earliest approaches to speech recognition were based on finding speech sounds and providing appropriate labels to these sounds. This is the basis of the acoustic phonetic approach (Hemdal and Hughes 1967). Which postulates that there exist finite, distinctive phonetic units (phonemes) in spoken language and that these units are broadly characterized by a set of acoustics properties that are manifested in the speech signal over time? Even though, the acoustic properties of phonetic units are highly variable, both with speakers and with neighboring sounds (the so-called co articulation effect), it is assumed in the acoustic-phonetic approach that the rules governing the variability are straightforward and can be readily learned by a machine [10].There are three techniques that have been applied to the language identification. Problem phone recognition, Gaussian mixture modeling, and support vector machine classification. The acoustic phonetic approach has not been widely used in most commercial applications.

2) Pattern Recognition approach

The pattern-matching approach (Itakura 1975; Rabiner 1989; Rabiner and Juang 1993) involves two essential steps namely, pattern training and pattern comparison. The essential feature of this approach is that it uses a well formulated mathematical framework and establishes consistent speech pattern representations, for reliable pattern comparison, from a set of labeled training samples via a formal training algorithm. A speech pattern representation can be in the form of a speech template or a statistical model (e.g., a HIDDEN MARKOV MODEL or HMM) and can be applied to a sound (smaller than a word), a word, or a phrase. In the pattern comparison stage of the approach, a direct comparison is made between the unknown speeches (the speech to be recognized) with each possible pattern learned in the training stage in order to determine the identity of the unknown according to the goodness of match of the

patterns [6].

2) Template based approaches

Template based approaches matching (Rabiner et al., 1979) unknown speech is compared against a set of pre-recorded words (templates) in order to find the best match. This has the advantage of using perfectly accurate word models. Recognition is carried out by matching an unknown spoken utterance with each of these reference templates and selecting the category of the best matching pattern. Usually templates for entire words are constructed. One key idea in template method is to derive a typical sequence of speech frames for a pattern (a word) via some averaging procedure, and to rely on the use of local spectral distance measures to compare patterns. Another key idea is to use some form of dynamic programming to temporarily align patterns to account for differences in speaking rates across talkers as well as across repetitions of the word by the same talker. [7].

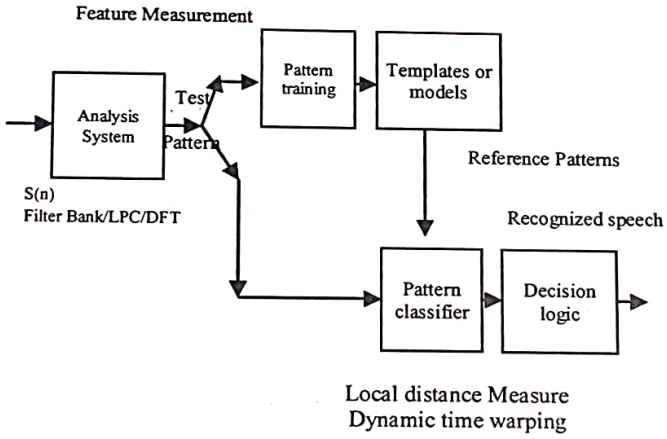


Fig.3 Block diagram of Pattern recognition

3) Dynamic Time Warping (DTW)

Dynamic time warping is an algorithm for measuring similarity between two sequences which may vary in time or speed. For instance, similarities in walking patterns would be detected, even if in one video, the person was walking slowly and if in another, he or she was walking more quickly, or even if there were accelerations and decelerations during the course of one observation. DTW has been applied to video, audio, and graphics indeed. Any data which can be turned into a linear representation can be analyzed with DTW. In general, DTW is a method that allows a computer to find an optimal match between two given sequences (e.g. time series) with certain restrictions. The sequences are "warped" non-linearly in the time dimension to determine a measure of their similarity independent of certain non-linear variations in the time dimension. This sequence alignment method is often used in the context of hidden Markov models. Continuity is less important in DTW than in other pattern matching algorithms. This technique is quite efficient for isolated word recognition and can be modified to recognize connected word also [8].

5) Knowledge Based Approach Knowledge

Knowledge based approach uses the information regarding linguistic, phonetic and spectrogram. Some speech researchers developed recognition system that used acoustic phonetic knowledge to develop classification rules for speech sounds. Vector Quantization (VQ) [9] is often applied to ASR. It is useful for speech coders, i.e., efficient data reduction. The utility of VQ here lies in the efficiency of using compact codebooks for reference models and codebook searcher in place of more costly evaluation methods. The test speech is evaluated by all codebooks and ASR chooses the word whose codebook yields the lowest distance measure. Knowledge has also been used to guide the design of the models and algorithms of other techniques such as template matching and stochastic modeling. This form of knowledge application makes an important distinction between knowledge and algorithms. Algorithms enable us to solve problems. Knowledge enables the algorithms to work better. It plays an important role in the selection of a suitable input representation, the definition of units of speech, or the design of the recognition algorithm itself.

6) The Artificial Intelligence Approach

The Artificial Intelligence approach [10] is a hybrid of the acoustic phonetic approach and pattern recognition approach. In this, it exploits the ideas and concepts of Acoustic phonetic and pattern recognition methods. The artificial intelligence approach attempts to mechanize the recognition procedure according to the way a person applies its intelligence in visualizing, analyzing, and finally making a decision on the measured acoustic features.

A large body of linguistic and phonetic literature provided insights and understanding to human speech processing this knowledge is usually derived from careful study of spectrograms and is incorporated using rules or procedures. In more indirect forms, knowledge has also been used to guide the design of the models and algorithms of other techniques, such as template matching and stochastic modeling. This form of knowledge application makes an important distinction between knowledge and algorithms.

7) Statistical Based Approach

In this approach, variations in speech are modeled statistically (e.g., HMM), using automatic learning procedures. This approach represents the current state of the art. Modern general-purpose speech recognition systems are based on statistical acoustic and language models. Effective acoustic and language models for ASR in unrestricted domain require large amount of acoustic and linguistic data for parameter estimation. Processing of large amounts of training data is a key element in the development of an effective ASR technology now a days. The main disadvantage of statistical models is that they must make *a priori* modeling assumptions, which are liable to be inaccurate, handicapping the system's performance.

This new approach is a radical departure from the current HMM-based statistical modeling approaches. For text independents speaker recognition use left-right HMM for identifying the speaker from simple data and also HMM having advantages based on Neural Network and Vector Quantization. The HMM is popular statistical tool for modeling a wide range of time series data. In Speech recognition area, HMM have been applied with great success to problem as part of speech classification [11]. The K-means algorithm is also used for statistical and clustering algorithm of speech Based on the attribute of data .The K in K-means represents the number of clusters the algorithm should return in the end. As the algorithm starts K points known as cancroids are added to the data space. The K-means algorithm is a way to cluster the training vectors to get feature vectors. In this algorithm clustered the vectors based on attributes into k partitions. It uses the k means of data generated from Gaussian distributions to cluster the vectors. The objective of the k-means is to minimize total intra-cluster variance.

8) Stochastic Approach

Stochastic modeling [12] entails the use of probabilistic models to deal with uncertain or incomplete information. In speech recognition, uncertainty and incompleteness arise from many sources; for example, confusable sounds, speaker variability's, contextual effects, and homophones words. Thus, stochastic models are particularly suitable approach to speech recognition. The most popular stochastic approach today is hidden Markov modeling. A hidden Markov model is characterized by a finite state Markov model and a set of output distributions. The transition parameters in the Markov chain models, temporal variability's, while the parameters in the output distribution model, spectral variability's. These two types of variability's are the essence of speech recognition. Compared to template based approach,

Hidden Markov modeling is more general and has a firmer mathematical foundation. A template based model is simply a continuous [12].

D. MATCHING TECHNIQUES

Speech-recognition engines match a detected word to a known word using one of the following techniques (Svendsen et al., 1989)

1) Whole-word matching:

The engine compares the incoming digital-audio signal against a pre-recorded template of the word This technique takes much less processing than sub-word matching, but it requires that the user (or someone) prerecord every word that will be recognized - sometimes several thousand words. Whole-word templates also require large amounts of storage (between 50 and 512 bytes per word) and are practical only if the recognition vocabulary is known when the application is developed [13].

2) Sub-word matching:

The engine looks for sub-words – usually phonemes and then performs further pattern recognition on those. This technique takes more processing than whole-word matching, but it requires much less storage (between 5 and 20 bytes perword). In addition, the pronunciation of the word can be guessed from English text without requiring the user to speak the word beforehand [14] [15].

TABLE I
RESULTS OBTAINED USING DIFFERENT FEATURE EXTRACTION AND MATCHING TECHNIQUE

Author	Year	Research Work	Nature of Data	Feature Extraction Technique	Feature Matching Technique	Language	Accuracy
Ghulam Muhammad, Yousef A. Alotaibi, and Mohammad Nurul Huda	2009	Automatic Speech Recognition for Bangia Digits	Small vocabulary Speaker independe nt Isolated digit	Mel-Frequency Cepstral Coefficient s (MFCCs)	Hidden Markov Model (HMM)	Bangia	more than 95% for digits (0-5) and less than 90% for digits (6-9)
Corneliu Octavian Dumitru, Inge Gavat	2006	A Comparative Study of Feature Extraction Methods Applied to Continuous Speech Recognition in Romanian Language	Large vocabulary Speaker independe nt Continuou s speech	PLP, MFCC, LPC	Hidden Markov Models (HMM)	Romanian	MFCC-90,41%, LPC-63,55%. and PLP 75,78%
Bassam A. Q. Al-Qatab , Raja N. Ainon	Arabic Speech Recogn ition Using Hidden Marko v Model Toolkit (HTK)	MFCC	HMM	Arabic	97.99%	Bassam A. Q. Al-Qatab , Raja N. Ainon	Arabic Speech Recogniti on Using Hidden Markov Model Toolkit (HTK)
M.Chandrasek ar, and M.Ponnavaiko	2008	Tamil speech recognition: a complete model	Medium vocabulary Speaker dependent Isolated Speech	MFCC	Back-Propagatio n Network	Tamil	80.95 %

III. PERFORMANCE OF A SYSTEM

For the performance analysis of the system, the following parameters will be considered for accuracy and speed measurement of the system.

1. Word Error Rate : $WER = (S + D + I)/N$
Where S is the number of substitutions, D is the number of deletions and I is number of insertions and N is the number of words in the reference speech sample.
2. Word Recognition Rate : $WRR = 1 - WER$
3. Real Time Factor : $RTF = P/I$ It takes time P to process an input of duration I.

IV. CONCLUSION

In this review, the fundamentals of speech recognition are discussed and its recent progress is investigated. The various approaches available for developing an ASR system are clearly explained with its merits and demerits. The performance of the ASR system based on the adopted feature extraction technique and the speech recognition approach for the particular language is compared in this paper. In recent years, the need for speech recognition research based on large vocabulary speaker independent continuous speech has highly increased. Based on the review, the potent advantage of HMM approach along with MFCC features is more suitable for these requirements and offers good recognition result.

FUTURE SCOPE

These techniques will enable us to create increasingly powerful systems, deployable on a worldwide basis in future. Results indicate that there is still room for recognition rate improvements. Using ANN technique these results can be increased further. Future work will focus on better selection of word groups and using speaker-dependent word groups.

REFERENCES

[1] Lawrence Rabiner, Biing Hwang Juang, Fundamental of Speech Recognition, Copyright 1999 by AT&T.

[2] GIN-DER WU AND YING LEI " A Register Array based Low power FFT Processor for speech recognition" Department of Electrical engineering national Chi Nan university Puli545 Taiwan.

[3] B. Yegnanarayana, S.R.M. Prasanna, J. M. Zachariah, and C.S. Gupta, "Combining evidence from source, suprasegmental and spectral features for a fixed- text specker verification system," IEEE Trans. Speech Audio Process.,vol.13(4), pp. 575-82, July2005.

[4] N.Uma Maheswari, A.P.Kabilan, R.Venkatesh, "A Hybrid model of Neural Network Approach for Speaker independent Word Recognition", International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010 1793-8201.

[5] Satyanarayana "short segment analysis of speech for enhancement" institute of IIT Madras feb.2009

[6] C.S.Myers and L.R.Rabiner, A Level Building Dynamic Time Warping Algorithm for Connected Word Recognition, IEEE Trans. Acoustics, Speech Signal Proc.,ASSP-29:284-297,April 1981.

[7]H.Sakoe and S.Chiba, Dynamic programming algorithm optimization for spoken word recognition ,IEEE Trans. Acoustics, Speech, Signal Proc., ASSP-26(1).1978

[8] Santosh K.Gaikwad, Bharti W.Gawali and Pravin Yannawar, "A Review on Speech Recognition Technique", International Journal of Computer Applications (0975 – 8887) Volume 10– No.3, November 2010

[9] Keh-Yih Su et.al, Speech Recognition using weighted HMM and subspace IEEE Transactions on Audio, Speech and Language.

[10] R.K.Moore, Twenty things we still don t know about speech, Proc.CRIM/ FORWISS Workshop on Progress and Prospects of speech Research an Technology, 1994.

[11] Shigeru Katagiri et.al, A New hybrid algorithm for speech recognition based on HMM segmentation and learning Vector quantization, IEEE Transactions on Audio Speech and Language processing Vol.1, No.4

[12] M.Weintraub et.al, linguistic constraints in hidden markov Model based speech recognition, Proc.ICASSP, pp.699-702, 1989.

[13]S.katagiri, Speech Pattern recognition using Neural Networks.

[14]L. R .Rabiner and B.H.jaung," Fundamentals of Speech Recognition Prentice-Hall, Englewood Cliff, New Jersy, 1993

[15] D. R. Reddy, An Approach to Computer Speech Recognition by Direct Analysis of the Speech Wave, Tech. Report No.C549, Computer Science Dept., Stanford Univ., September 1966.

KIET IJCE

KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

NONACK in Wireless Ad Hoc Network

Trisha Mittal[1], Bijendra Kumar[2]
Department of Computer Engineering
Netaji Subhas Institute of Technology, University of Delhi
New Delhi, India
trisha.nsit@yahoo.com [1] bizender@hotmail.com [2]

Abstract— **A wireless ad hoc sensor network (WSN) is made up of a number of geographically spread apart sensors each with a reasonable amount of signal processing and data networking ability coupled with wireless communication. One of the major challenges wireless sensor networks face today is security. Denial of service (DoS) attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. This paper explores resource depletion attack in a cooperative manner and increasing traffic on the routing layer protocol. The ease of carrying out a NONACK (Noose Noose attack) and the difficulty in its detection makes all examined protocols very susceptible to it. The worst case scenarios can see an upsurge in the network-wide usage by a factor of $O(N^2)$, N being the number of network nodes.**

Keywords— **wireless ad hoc sensor network(WSN); Denial of service; attack;nodes; NONACK**

I. Introduction

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors[1].For WSNs become more and more crucial to the everyday functioning of people and organizations like military, wireless traffic, wireless surveillance, wireless parking lot, thus, availability faults become less tolerable. Wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks and many researches have been done to enhance survivability. Attacks can be categorized in two ways: active attacks and passive attacks. Attacks that try to alter the functioning of the resources of the system are termed as active attacks and those that only analyze the system's information but do not affect the functioning of its resources are termed as passive attacks. [2]. Modification, fabrication and jamming are some of the common DOS attacks which are active attacks. Resource depletion attack is also a DOS attack which depletes the nodes batteries. In this paper we will discuss how routing protocols, even those designed to be secure, lack protection from NONACK, since they drain the life from networks nodes and also increase the delay. NONACK works in a cooperative manner provided none of the two malicious nodes being active at a time and hence they are really tough to be detected.

II. Related Work

Many resource depletion and DOS attacks have been defined, evaluated, or mitigated on various layers. With the rapid growth of Implantable Medical Devices (IMDs), their security becomes a critical issue since the attacks on the devices may directly harm the patient. Typical IMDs have restricted resources in terms of energy, processing capability, and storage. The Resource Depletion (RD) attacks are able to quickly deplete the resources of an IMD, such as battery power, thus, RD attacks can reduce the lifetime of an IMD from several years to a few weeks [3].Among various security threats, those attacks which lead to random drainage of the energy level of sensors, immensely affect the low power sensor nodes, thus, leading to death of the nodes. One of the most dangerous types of attack is sleep deprivation, where the intruder targets to maximize the power consumption of sensor nodes; so that their lifetime is minimized [4]. Another way of reducing the sensor lifetime is by targeting the sensor node's power supply as done by denial-of-sleep attack. These attacks are capable of diminishing the sensor's lifetime from years to days [5]. A framework has been proposed in the paper for defending against denial-of-sleep attack and specific techniques have been provided that can counter each denial-of-sleep susceptibility.

One of the DOS attacks is Vampire attack which involves depletion of the life of a node that is part of the wireless network [11]. This paper delves into the topic of resource depletion attacks at the routing protocol layer which permanently immobilize a network by exhausting the battery power of the nodes. A malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes that forward the packet based on the included source route. Vampire attacks are not protocol-specific. These depend upon the characteristics of many popular classes of routing protocols. NONACK also introduce loops in the route resulting in DOS attack and resource depletion attack. NONACK is even harder to detect and cause much more delay while consuming the battery power of nodes.

III. Nonack

A. Description of NONACK

The goal of Denial of Service (DoS) attacks is to prevent availability of network services from their legitimate users [6] [7]. Its basic aim is prevention of authorized access to the resources or time delaying. DoS attack has different scenarios. First attack scenario targets the memory, storage space, or CPU of the service provider. Second attack scenario targets energy resources like the battery power of the service provider. The third scenario targets bandwidth. NONACK

attack targets the second scenario. All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, in which topology discovery is done at transmission time, and static protocols, in which topology discovery is done at initial setup phase, where topology change is handled by periodic rediscovery. We would be focusing on on-demand routing protocol as for now.

In our attack, adversaries force the packet to create routing loops before reaching to destination and the two adversaries work in a cooperative manner. We call it NONACK as shown in Fig. 1.

When one of the adversaries is performing NONACK, the other partner (adversary) will be behaving just as an honest node and we call it as its resting stage. First adversary will initiate the second one to create loops before going into rest mode and in this manner second adversary will again initiate first one before going to rest. In this way one of the two adversaries will be working whole the time provided the same node never work maliciously for the whole time and also the two will never behave malicious at the same time. Hence it becomes really very difficult to detect NONACK attack. The limited verification of message headers at forwarding nodes becomes the Achilles heel for the source routing protocol. During a NONACK a single packet is made to repeatedly traverse the same set of nodes until delivery to the destination. This will consume the battery life of all the nodes in the network.

The algorithm for the NONACK is given in Fig. 2.

B. *Assumptions*

We assume that only adversaries originated messages may have maliciously composed routes. Our adversaries are malicious insiders and the level of resource and network access is same as done by an honest node. Once the battery power is exhausted, the node will be permanently disabled. Initial energy level of network is 200 joules. We assume all the nodes have the same initial transmission range of 250 meters, traffic type is 512 bytes cbr, size of simulation area 1500*1500.

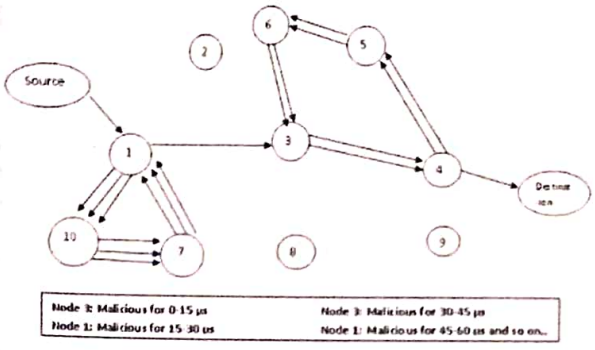


Fig. 1 NONACK

```
N<-node list;
s<- source_address;
d<- destination_address;
flag<-0;
select x<- routing protocol;
call route_discovery(s,d);
return posible_path_list;
executed_path=best_path(possible_path_list);
m1=pick_Malicious(executed_path_node_list) //choose a node m1 in executed path as malicious node
loop1=formloop(m1,(N-executed_path));
m2=pick_Malicious(executed_path_node_list- m1);
loop2=formloop(m2,(N-executed_path));
for(count=1;count<1000000;count+2) //total simulation time is 15 second and loop switches after every 15 microsec
{
if(flag==0)
        {
        executed_path=executed_path + loop1;
        delay(15) //(delay(time in microseconds))
        flag=1;
        executed_path=executed_path - loop1;
        }
        if(flag==1)
        {
        executed_path=executed_path + loop2;
        delay(15)
        flag=0;
        executed_path=executed_path - loop2
        }
}
```

Fig. 2 Algorithm of NONACK

IV. Simultion Of Nonack

We evaluated NONACK in a randomly generated 30 to 50 sensor node topology and DSR(Dynamic Source Routing) routing protocol and two randomly selected malicious DSR agents, using the ns-2 network simulator [8]. Mac 802.11 and Omni antenna is used for data communication and covering the transmission range. The routing is performed between sensor nodes, let the data packets be 512 bytes and the initial energy level of nodes be 100 joules. The graphical constraints like throughput, packet delivery ratio, delay are used to evaluate the performance of network.

A. *DSR*

DSR is a reactive routing protocol which does not use periodic table-update messages as done by table-driven

routing protocols [9]. DSR, specifically designed for use in multi-hop wireless ad hoc networks, allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets. Compared to other reactive routing protocols like Adhoc On Demand Distance Vector routing[10] and DSDV, DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence.

DSR is based on the Link-State-Algorithms which mean that each node is capable of saving the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding.

B. Path Selection And Loop Formation

In this case, Node–20 acts as source node and 45 acts as destination node, source node broadcast a RREQ message to reach destination, and destination replies RREP message to source through three paths,

- Priority path_1: 45-24-23-22-21-20
- Priority path_2: 45-46-30-29-28-27-26-20
- Priority path_3: 46-44-18-17-16-15-14-20

Source node selects the first priority path, since it has the minimum hop count and nearer distance. And source node 20 transmits data to destination through intermediate nodes 21-22-23-24, at certain time intermediate node 24 behave as a malicious node and forms a loop, in loop node 18-17-16-10-11-12-18 will be involved as shown in Fig. 3, then the packet is transmitted to destination, in addition another intermediate node 22 also forms a loop with nodes-28-34-35-29-28, and then the packets are transmitted to destination. Both the malicious node 24 and 22 forms a loop alternatively with the time interval of 15 micro sec, hence make energy consumption much larger, and affect the network performance.

V. Results and Comparison

NONACK is a more powerful and cooperative version of carousel attack mentioned in vampire attack [8]. In carousel basically only a single node make the loop but in NONACK two nodes perform this in cooperative manner and hence resulting in more damage in terms of delay, throughput and packet delivery ratio and even much different to find that exact which node is malicious.

A. Packet Delivery Fraction (PDF)

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

$$PDF = \frac{\text{Number of received packets}}{\text{Number of sent packets}}$$

The packet delivery ratio of the network in presence of NONACK is 79% and in presence of carousel is 94% as shown in Fig. 4.

Fig. 3 Simulation of NONACK

B. Average End-to-End Delay (AED):

The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges.

$$AED = \frac{\Sigma\,(\text{time received} - \text{time sent})}{\text{Total data packets received}}$$

The delay time is determined in presence of NONACK is 22 seconds and in presence of carousel is about 10 seconds as shown in Fig. 5.

C. Throughput

Total number of Bytes successfully transmitted from source to destination per second. It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

The throughput rate in presence of NONACK is 60 kb/s and in presence of carousel attack is 80 kb/s destination as shown in Fig. 6.

D. Packet loss

Packet loss is the failure of one or more transmitted packets to arrive at their destination. The packet loss determined as in presence of NONACK is 26 and in presence of carousel is 18 as shown in Fig. 7.

E. Energy consumption

Energy required for transmitting a packet from source to destination.

The energy consumption of NONACK is 85 joules and for carousel attack is 65 joules as shown in Fig. 8.

The energy consumption in normal data transfer, in presence of NONACK and in case of carousel attack is shown in Fig. 9.

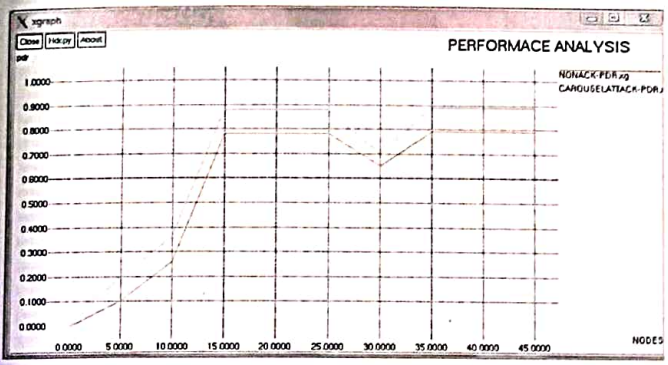


Fig. 4 PDR simulation results for NONACK and carousel attack

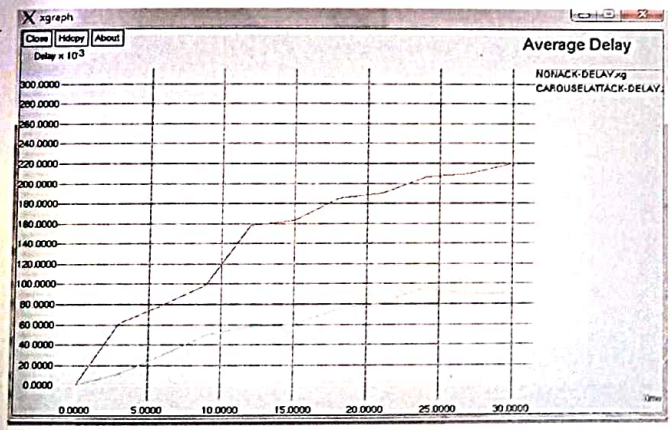


Fig. 5 AED simulation results for NONACK and CARUSOAL attack

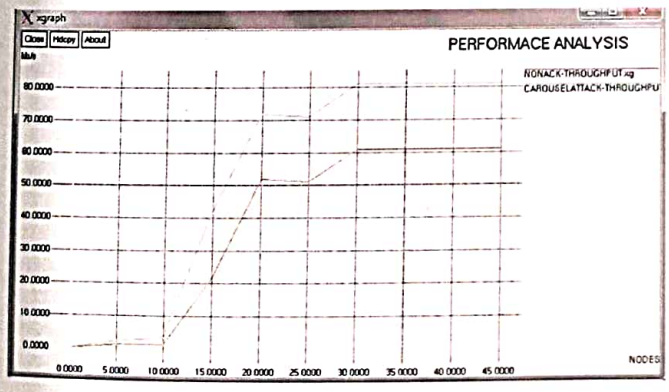


Fig. 6 Throughput simulation results for NONACK and carousel attack

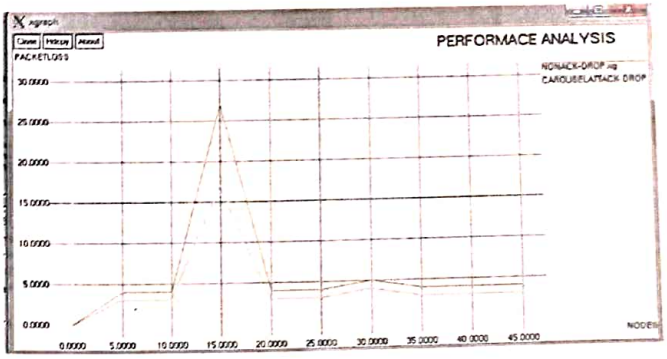


Fig. 7 Packet loss simulation results for NONACK and carousel attack

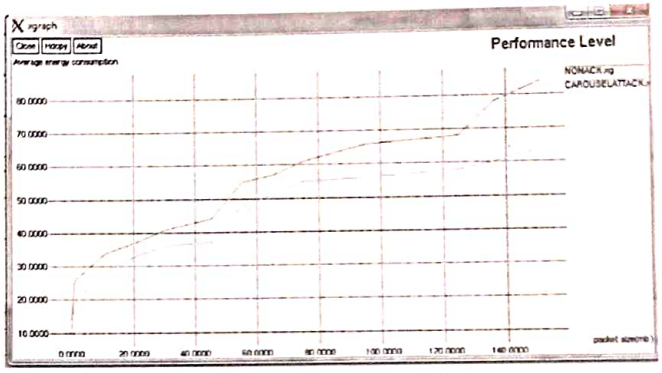


Fig. 8 Average energy consumption in presence of NONACK and carousel attack.

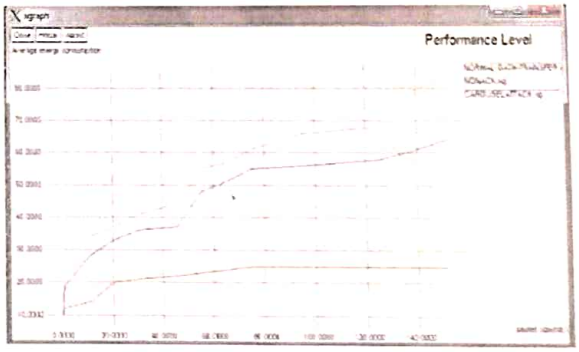


Fig. 9 Average energy consumption in case of normal data transfer and in presence of NONACK and carousel attack.

VI. Conclusion

In this paper, we have defined NONACK as a resource consumption attack that disables ad hoc wireless sensor networks by exhausting the battery power of the member nodes by using the routing protocol. This also results in delivery delay as the packet first revolves in loop before going to destination. Simulation results show that NONACK results in almost double end-to-end delay in comparison with carousel attack of vampire. Also it results in higher energy consumption and low throughput.

We will try to give a solution for this attack as the future work.

REFERENCES

[1] Eiko Yoneki, Jean Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role", University of Cambridge Computer Laboratory,Cambridge CB3 0FD, United Kingdom, September 2005.

[2] "What is Active Attack?" available at http://en.wikipedia.org/wiki/Attack_%28computing%29.

[3] Xiali Hei, Xiaojiang Du," The Resource Depletion Attack and Defense Scheme", SpringerBriefs in Computer Science 2013, pp 9-18

[4] Tapalina Bhattasali ,Rituparna Chaki ,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887),Volume 40– No.15, February 2012

[5] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,"IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[6] Kemal Bicakci,Bulent Talavi,"Denial-of-Service attacks and countermeasures in IEEE wireless networks,"Computer Standards & Interfaces 31 (2009) 931-941

[7] Imad Aad,Jean-Pierre Haubaux,Edward W.Knightly, "Impact of Denial of service attacks on Ad Hoc Networks ".

[8] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.

[9] David B. Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks" http://www.monarch.cs.cmu.edu/

[10] "Mobile Ad hoc Networking (MANET) with AODV", available at http://www.cs.virginia.edu/~jwang/STIL_files/NovaRoam_documents/AODV%20White%20Paper.pdf

[11] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", Published by the IEEE CS, CASS, ComSoc, IES, & SPS, 2013.

KIET IJCE International Journal of Communications & Electronics
Volume. 2, Issue No. 2, July-Oct 2014

An Improved W-CMSR for Direction Of Arrival Estimation

Amit Verma[1], Sandeep Santosh[2]
Department of Electronics Engineering,
National Institute of Technology, Kurukshetr, Kurukshetra-136119, India
amit.verma7007@gmail.com[1], profsandeepkkr@gmail.com[2]

Abstract— **In this paper, an improved W-CMSR method for direction-of-arrival estimation for wideband signal is proposed. An important parameter in direction of arrival estimation by W-CMSR is the fitting error threshold. The accuracy and the angular resolution for direction of arrival estimation hugely depends on this fitting error threshold. This paper propose a method to calculate the fitting error threshold in a way that angular resolution for estimation as well as accuracy of estimation improves. Also the complexity of the proposed method is lesser than the conventional W-CMSR method.**

Keywords— ***Direction-of-arrival estimation, sensor array, wideband signals, W-CMSR***

I. Introduction

Direction-of-arrival (DOA) denotes the direction from which an unknown incoming wave impinges on the sensor array. The basic device for the direction-of-arrival estimation is the sensor arrays. These sensor arrays are formed by spatially placing the multiple sensor in a desired manner as per the requirement. The spatial arrangement can be linearly, circularly or any other manner in a uniform or non-uniform way as per the requirement.

The direction-of-arrival estimation is an important research area as many application like finding sound source, multi user wireless communication, localizing target by radar, sonar and many more require the accurate information about the direction of the incoming propagating wave. Many techniques has been proposed in past to estimate the direction-of-arrival estimation of the wideband signals such as Music method [1], L1-SVD [2], JLZA [3] and so forth. Most of those method requires the spectral decomposition of the incident signal to estimate the direction of the incoming signals. Method of these category has disadvantage that these method require pre-estimate of the incident signals for the spectral focusing and the accuracy of such pre-estimates largely effects the performance of the system in terms of accuracy and angular resolution. Such method also require the a priori information about the number of signal impinging on the sensor array. Practically, these information are not available for direction-of-arrival estimation. The method of W-CMSR [4] does not require the spectral decomposition of the incoming wideband signals into narrowband signals [5] as well as it does not require any priori information about the number of incoming signals. These advantages of W-CMSR over other method made it popular for direction-of-arrival estimation. In W-CMSR, the lower half element of the covariance matrix are aligned to form a measurement vector. This measurement vector is reconstructed over complete dictionary to perform the direction-of-arrival estimation. The a priori information about the number of sources is not required in this kind of representation and hence this method has a certain advantage over the other method. Also such representation do not break down the incoming wideband signals into narrowband signal and evaluate the incoming signals integrated and therefore reduces the complexity in the estimation process. The restriction for the half wavelength for avoiding uncertainty is eased to lower frequency from higher frequency for this method. This method has the ability to estimate direction-of-arrival of more number of signals than sensors for a well-designed geometry. This paper improves the method of W-CMSR by modifying the fitting error threshold for the direction- of-arrival estimation.

This paper consist of following sections. Section II presents the basic wideband direction-of-arrival model. Section III presents the model of W-CMSR. Section IV discuss the proposed method whereas simulation results are demonstrated in section V. The final conclusions are made in section VI. Section VII consists of the references.

II. Problem Formulation

Consider that W sources are transmitting the wideband signals from the direction $\Phi_1, \Phi_2 \ldots \Phi_w$. These signal impinges on the array of sensors consisting of N sensors. The output at each sensor is given by

$$x_n(t) = \sum_{w=1}^{W} s_w(t + \tau_{n,w}) + \sigma_n(t) \qquad (1)$$

where σ_n is the additive noise at the n^{th} sensor and s_w is the w^{th} signal arriving at the n^{th} sensor with the propagation delay of $\tau_{n,w}$.

Assuming that Q snapshots are collected, the output of sensors array at time t is given by

$$x(t) = \left[\sum_{w=1}^{W} s_w(t + \tau_{1,w}) + \sigma_1(t), \ldots, \sum_{w=1}^{W} s_w(t + \tau_{n,w}) + \sigma_n(t) \right]^T \qquad (2)$$

Since the wideband signals have the substantial bandwidth, hence the propagation delay of incoming signal in (1) cannot be converted into phase delay.

III. W-CMSR METHOD

The direction-of-arrival of the wideband signal presented in this section is based on the correlation functions of wideband signals. This correlation function can be extracted from the covariance matrix of the array output.

Assuming the unified correlation function of the incoming signals to be analogous, i.e

$$r_{w_1}(\tau) = r_{w_2}(\tau) \forall w_1, w_2 \in [1,....W] \quad (3)$$

The perturbation free covariance matrix is given by

$$C = \begin{matrix} \sum_{w=1}^{W} \rho_w + \eta_\sigma^2 & \sum_{w=1}^{W} \rho_w r^*(\tau_{2,w} - \tau_{1,w}) & \cdots & \sum_{w=1}^{W} \rho_w r^*(\tau_{N,w} - \tau_{1,w}) \\ \sum_{w=1}^{W} \rho_w r(\tau_{2,w} - \tau_{1,w}) & \sum_{w=1}^{W} \rho_w + \eta_\sigma^2 & \cdots & \sum_{w=1}^{W} \rho_w r^*(\tau_{N,w} - \tau_{2,w}) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{w=1}^{W} \rho_w r(\tau_{N,w} - \tau_{1,w}) & \sum_{w=1}^{W} \rho_w r(\tau_{N,w} - \tau_{2,w}) & \cdots & \sum_{w=1}^{W} \rho_w + \eta_\sigma^2 \end{matrix} \quad (4)$$

where ρ_w is the power of w^{th} signal and η_σ^2 is the variance of additive noise.

The direction-of-arrival of the incoming signals can be estimated from the correlation function family of $r(\tau_{i,w} - \tau_{j,w})$ for each w where $i,j = 1,2,....,N$ but each element of the covariance matrix contains W correlation and diagonal element of the covariance matrix is polluted by the noise variance which is unknown and hence estimation of direction-of-arrival cannot be performed from covariance matrix directly.

It is clear from the (4) that elements above and below the main diagonal of covariance matrix are conjugate to each other and therefore only lower left triangular element is enough to represent the covariance matrix.

Since the diagonal elements are polluted by noise, hence aligning lower left elements column-by-column to form a new one-dimension measurement vector m given by

$$m = \left[C_{2,1},....,C_{N,1},C_{3,2},...,C_{N,2},...,C_{N,N-2},C_{N,N-1}\right]^T \quad (5)$$

where $C_{n1,n2}$ represents $(n_1,n_2)^{th}$ element of Covariance matrix, C.

This vector can also be written as

$$m = \sum_{w=1}^{W} \rho_w k_w \quad (6)$$

where

$$k_w = \left[r(\tau_{2,w} - \tau_{1,w}),...,r(\tau_{N,w} - \tau_{1,w}),...,r(\tau_{N,w} - \tau_{N-1,w})\right] \quad (7)$$

The incoming signal elements coming from the certain directions depend on the unified correlation function. Thus, if the signal elements can be separated then the signal directions can be estimated from m. Considering $\tau_n^{(\phi)}$ be the propagation delay of incoming signal from direction ϕ from reference point to n^{th} sensor then signal elements with unit power is given by

$$m^{(\phi)} = \left[r(\tau_2^{(\phi)} - \tau_1^{(\phi)}),...,r(\tau_N^{(\phi)} - \tau_1^{(\phi)}),...,r(\tau_N^{(\phi)} - \tau_{N-1}^{(\phi)})\right]^T \quad (8)$$

Now, consider the angular grid for incident signal to generate the direction set α. For e.g., if we consider the interval of δ for the angular grid between -90° to +90° then the direction set is given by

$$\alpha = \left[-90^o, -90^o + \delta, ..., +90^o\right] \quad (9)$$

Thus m can be formulated over complete angular grid as

$$m = m^{(\alpha)}\rho \quad (10)$$

where ρ is the sparse vector having non-zero values. ρ_w (w = 0,1,....,W) indexed matching to the signal direction location in α.

The solution of (10) imposing sparsity is given by

$$\hat{\rho} = \arg\min_{\rho} \| \rho \|_0, \text{ subject to } m = m^{(\alpha)}\rho \quad (11)$$

where $\hat{\rho}$ denotes the spatial distribution of the incident signals and $\| \|_0$ indicates the L0-norm [6].

From (8), it is evident that dictionary elements depends on the correlation function [7] of the incident signals and hence we will first calculate the correlation function.

The correlation function is given by

$$r(\tau) = \frac{1}{P_I}\int_\sigma P(\omega)e^{j\omega\tau}d\omega \quad (12)$$

where $P_I = \int_\sigma P(\omega)d\omega$ and the integral scope σ is fixed according to bandwidth of signal. $P(\omega)$ denotes the signal power spectrum. Output of the sensor array can be used to estimate the power spectrum of signal.

The above model in (11) does not consider the agitations in the practical environment. Considering the agitations in the practical environment, we convert L0-norm based problem in (11) into L1-norm optimization problem.

$$\hat{\rho} = \arg\min_{\rho} \| \rho \|_1, \text{ subject to} \| m - m^{(\alpha)} \rho \|_2 \leq \beta \tag{13}$$

where fitting error, β is given by [4][8]

$$\beta = \mu \times \left\{ \frac{N(N-1)}{2Q} \left[\Xi \left(\sum_{w=1}^{W} \rho_w \right)^2 + 2\eta_\sigma^2 \left(\sum_{w=1}^{W} \rho_w \right) + \eta_\sigma^4 \right] \right\}^{\frac{1}{2}} \tag{14}$$

where μ is the weighting factor and Ξ is given by

$$\Xi = \sum_{\Delta t = qT_s} |r(\Delta t)|^2 \tag{15}$$

To test the performance of the W-CMSR, we consider two BPSK signals arriving at the sensor array from different angle. During the experiment, we consider 7 sensor uniform linear array (ULA) with half wavelength spacing between the sensor elements.

Fig. 1., Fig. 2., Fig. 3. and Fig. 4. shows that the W-CMSR method is able to detect the incoming signal. In the experiment, two signals are taken with direction of first signal is fixed to 20° and the direction of second signal is varied from 45° to 30° with difference of 5° between them.

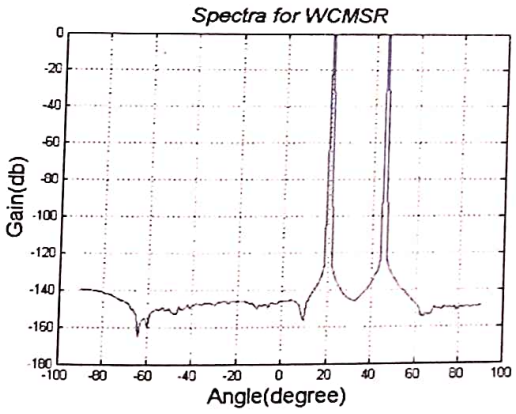


Fig. 1 Spectra of W-CMSR when DOA of signals are 20^0 and 45^0

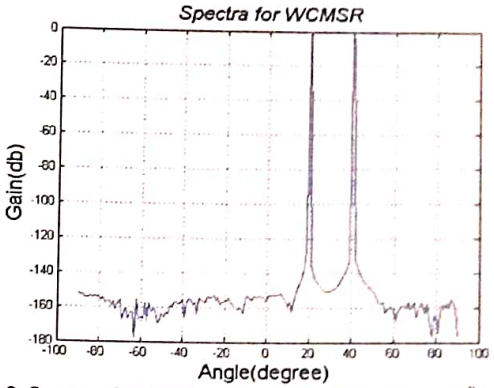


Fig. 2 Spectra of W-CMSR when DOA of signals are 20^0 and 40^0

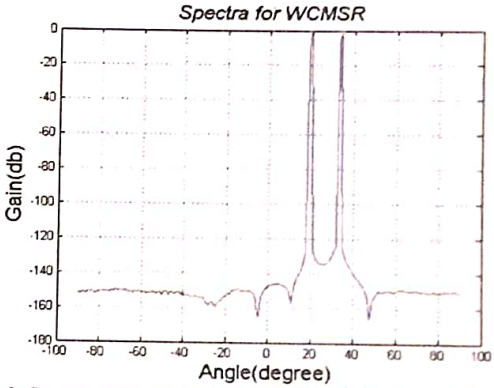


Fig. 3 Spectra of W-CMSR when DOA of signals are 20^0 and 35^0

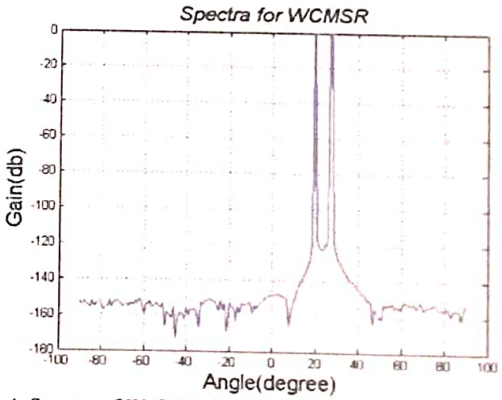


Fig. 4 Spectra of W-CMSR when DOA of signals are 20^0 and 30^0

IV. Proposed Method

The calculation of fitting error plays the vital role in the accuracy and angular resolution of direction-of-arrival estimation. In this paper, we propose a method to calculate the fitting error in a manner so that accuracy as well as the angular resolution of the W-CMSR method improves. The proper selection of fitting error has the huge impact on feasibility and efficiency of (13).

In this method, we calculate the covariance matrix by two method and then align them to get the two correlation function. The absolute difference between these correlation function is

called as residual error. This residual error is used to calculate the fitting error threshold.

The first covariance matrix is calculated as follows

$$R = \frac{1}{Q} * X * X^T \tag{16}$$

where X is given by

$$X = \left[\sum_{w=1}^{W} s_w(t+\tau_{1,w}) + \sigma_1(t), \ldots, \sum_{w=1}^{W} s_w(t+\tau_{n,w}) + \sigma_n(t) \right]^T_{t=1\ldots\ldots Q} \tag{17}$$

The matrix X is called the array output matrix which contains Q snapshots of the output of sensor arrays. Now we align the lower half triangular element of matrix R to obtain a new measurement vector M_1.

$$M_1 = \left[R_{2,1}, \ldots, R_{N,1}, R_{3,2}, \ldots, R_{N,2}, \ldots, R_{N,N-2}, R_{N,N-1} \right]^T \tag{18}$$

The mean of each row of matrix X gives the approximate value of sensor output. Let the mean matrix be denoted by Y and thereby second covariance matrix is calculated as follows

$$S = \frac{1}{Q} * Y * Y^T \tag{19}$$

Aligning the lower half triangular element of matrix S to obtain a measurement vector M_2.

$$M_2 = \left[S_{2,1}, \ldots, S_{N,1}, S_{3,2}, \ldots, S_{N,2}, \ldots, S_{N,N-2}, S_{N,N-1} \right]^T \tag{20}$$

The absolute difference of M_1 and M_2 is called the residual error and is given by

$$m_p = abs(M_1 - M_2) \tag{21}$$

where abs denotes the absolute value of the argument in bracket.

Finally, the fitting error threshold depends on this residual error and this fitting error, β is given by

$$\beta = \frac{3.5}{[geomean(m_p)]^{1/3.5}(W-1)} \tag{22}$$

where geomean(m_p) is the geometric mean of the m_p and W as described above is the number of wideband signals impinging on the sensor array.

V. Simulation Results

This section shows the performance of the proposed method and compare it with the W-CMSR method. In the simulation, sensor array of seven sensor is taken having half wavelength as the spacing between the sensors.

The Sensor number can be varied according to the requirement but the accuracy of method strongly depends upon the optimum selection of sensor number. The number of sensors can be reduced at the cost of accuracy. Sedum is used as the optimization tool to solve the problem in (13). The angular grid as described in (9) is taken as [-90° +90°] in all the experiments with 1° interval between them.

In fig. 5 we have taken two incoming signals arriving from the direction of 20°and 25°. It can be seen in the fig. 5. that both proposed method and W-CMSR method are unable to estimate the direction of incoming signals. Both the method is only able to estimate the direction of incoming signal arriving at angle of 20^0 with the bias of 1^0. This also clears the fact that both the methods have certain minimum angular separation beyond which the signals cannot be separated.

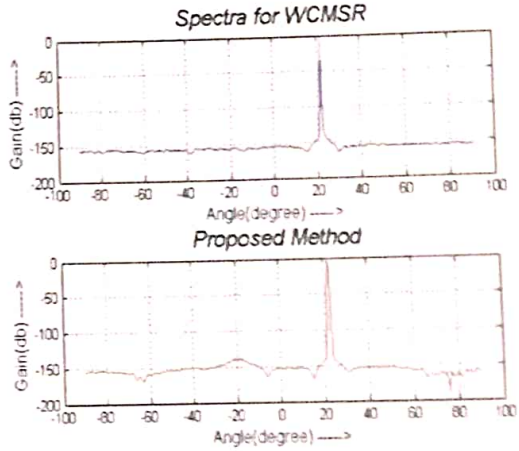


Fig. 5 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 25^0

In fig. 6 we have taken two incoming signals arriving from the direction of 20°and 26°.It is clear from fig. 6 that the proposed method is able to detect the incoming signals from angle of 20^0 and 26° whereas the previous method is unable to detect the direction of incoming signals and is only able to detect the signal incoming from 20^0.

Another result that can be reached from above experiment is that the angular separation between two signals must be at least 6° so that the two signals can be successfully detected by proposed method.

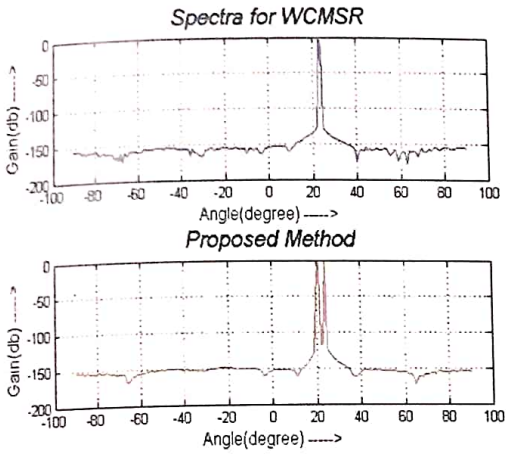


Fig. 6 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 26^0

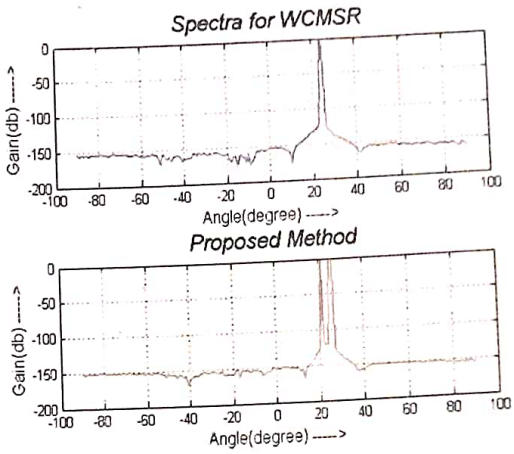


Fig. 8 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 28^0

Similar to the previous case. It is clear from fig. 7. and fig. 8. that the proposed method is able to detect the incoming signals from angle of 20^0 and 27° or 20^0 and 28° respectively whereas the W-CMSR method is unable to detect the direction of incoming signals and is only able to detect the signal incoming from 20^0.

Fig. 9. and Fig. 10. shows that both the method are able to detect the incoming signal from 20^0 and 29° or 20^0 and 30° respectively. It can also be concluded thatthe angular separation between two signals must be at least 9° so that the two signals can be successfully detected by W-CMSR method.

It can be seen from all the experiment conducted that the angular resolution of the proposed method is better than that of the previous method.

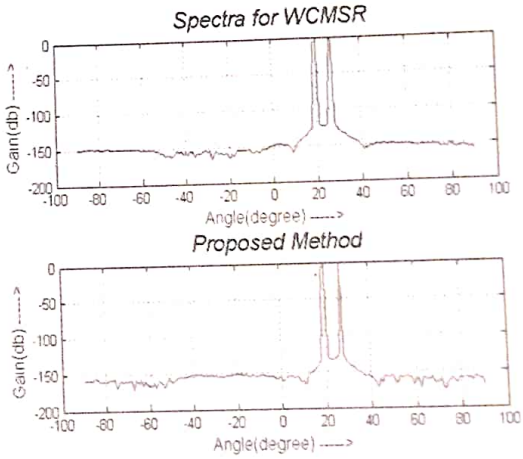


Fig. 9 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 29^0

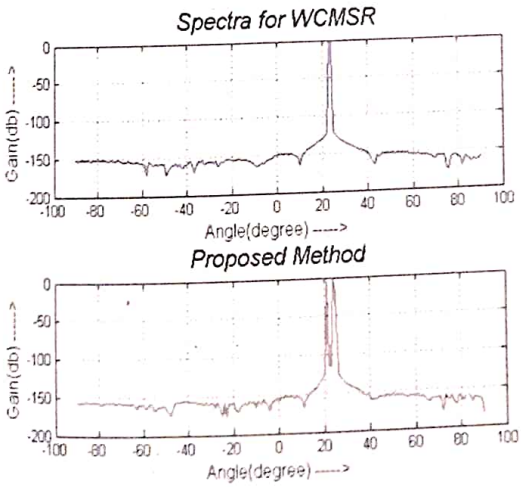


Fig. 7 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 27^0

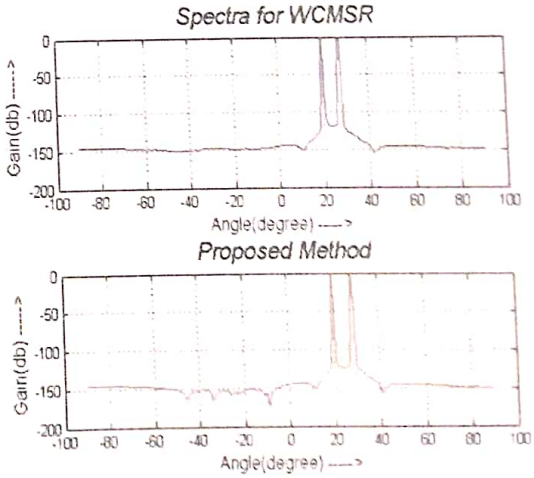


Fig. 10 Spectra of proposed W-CMSR when DOA of signals are 20^0 and 30^0

VI. Conclusion

An improved W-CMSR for wideband direction of arrival estimation is proposed in this paper. The advantage of W-CMSR method over other direction of arrival estimation methods as well as the role of fitting error threshold on the accuracy and angular resolution of estimation is discussed. A method to calculate the fitting error is developed. The simulation results show that the angular resolution of the proposed method is better than that of the W-CMSR method. The Simulation further shows that the new value of fitting error threshold not only improves the angular resolution of the estimation but also improves the accuracy of the estimation method.

REFERENCES

[1] Ralph O. Schmidt, "Multiple Emitter Location and Signal Parameter Estimation," IEEE Transaction on Antennas and Propagation, AP, vol. 34, no. 3, March 1986.

[2] D. Malioutov, M. Cetin, and A. S. Willsky, "A sparse signal reconstruction perspective for source localization with sensor arrays," IEEE Trans. Signal Process., vol. 53, no. 8, pp. 3010–3022, Aug. 2005.

[3] [3] M. M. Hyder and K. Mahata, "Direction-of-arrival estimation using a mixed L2,0 norm approximation," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4646–4655, Sep. 2010.

[4] Zhang-Meng Liu, "Direction-of-Arrival Estimation of Wideband Signals via Covariance Matrix Sparse Representation" IEEE Transactions On Signal Processing, Vol. 59, No. 9, September 2011.

[5] H. Krim and M. Viberg, "Two decades of array signal processing research:The parametric approach," IEEE Signal Process. Mag., vol. 13, no. 4, pp. 67–94, Jul. 1996.

[6] B. K. Natarajan, "Sparse approximate solutions to linear systems," SIAM J. Comput., vol. 24, pp. 227–234, 1995.

[7] B. P. Lathi, Signal Processing and Linear Systems. London, U.K.: Oxford Univ. Press, 1998.

[8] D. L. Donoho, S. Mallat, R. Sachs, and Y. Samuelides, "Locally stationary covariance and signal estimation with macrotiles," IEEE Trans. Signal Process., vol. 51, no. 3, pp. 614–627, Mar. 2003.

KIET IJCE KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

A Review on Quantum-dot Cellular Automata Memory Circuits

[1]Deepmala Srivastava, [2]Dr. Rabindra Kumar Singh
Electronics Engineering Department,
Babu Banarsi Das Northern India Institute of Technology , Lucknow,
Kamla Nehru Institute of Technology, Sultanpur
[1]srvdeepmala@gmail.com, [2]singhrabinder57@gmail.com

Abstracts- CMOS technology presents some unsolved problems after shrinking certain limits. Thus for solve these problems new devices developed in place of CMOS in nanoscale era. These problems point to the need for a new kind of fundamental device and architecture, such as quantum-dot cellular automata (QCA). A QCA technology is quite different from CMOS technology. This changes the cost landscape which in turn changes the look of efficient designs. By using nanoelectronics devices like QCA it will be possible to produce high performance logic and memory integrated circuits in a small area. This paper reviewed the basics of QCA and its use in memory circuits.

Key Words-QCA, memory, clock, scaling

INTRODUCTION

Since the beginning of the seventies, the microelectronics industry has followed Moore's law, doubling processing power every 18 months. This performance increase has been obtained mainly by decreasing the size of circuit features obtained by optimization and improvement of existing technology. The current projections by the International Technology Roadmap for Semiconductors (ITRS) say that the end of the road on MOSFET scaling will arrive sometime around 2018 with a 22nm process [1]. Even getting to 22 nm presents some major unsolved hurdles. These are increasing power consumption, particularly through leakage currents, less tolerance for process variation, and increasing cost. Physical limits (quantum effects and non-deterministic behavior of small currents) and technological limits (such as power dissipation, design complexity and tunneling currents) may hinder the further progress of microelectronics on the basis of conventional circuit scaling. Quantum-dot cellular automata (QCA) is a potentially promising technology as an alternative to complementary-metal-oxide semiconductor (CMOS) technology for nanoscale device implementations.

Quantum-dot Cellular Automata (QCA) provides a new functional paradigm for information processing and communication. The main feature of this technology is the so-called processing-in-wire mechanism by which data movement and manipulation are strictly integrated. In this context, the design of memory devices is particularly challenging and interesting because the conventional storage arrangements applicable to CMOS based memories cannot be applied and innovative approaches must be used. The first section explain the basics of the QCA and then discussed some previous QCA based memory architecture and cell.

II.QCA BASICS

A lot of research has been done in the QCA devices because of its ability to go past the physical size limits of the CMOS devices [1, 2]. This includes work at circuit level as well as at device level.

Quantum-dot cellular automata (QCA) [3,4] have been proposed for implementing high performance digital circuits with low power consumption, very high density and fast operational speed [5] in nano scale era. QCA has many powerful features some of which are not available in CMOS [1][6]. Although many fabrication challenges have still to be overcome [6][7]. The simple design nature of QCA makes it attractive for investigation of new circuit topologies [8,9,10,11]. QCA topologies are not simple translations of standard circuit layouts; new ideas for translating standard logic units into QCA are needed. One of the interesting features of QCA is that there is no fixed connection strategy, and hence, it should be possible to apply optimization algorithms such as genetic algorithms to minimize the number of cells in a design.

QCA and the QCA cell was first introduced by Prof. C. S. Lent at the University of Notre Dame [3]. Quantum Dot consist of nanoscale crystals from a special class of

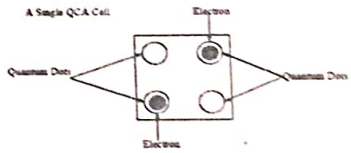


Figure 1 Single Quntum Cell

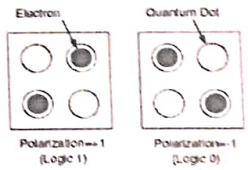


Figure 2 Representation of logic 1 and 0 in QCA Cell

semiconductor materials, which are crystals composed of chemical elements in the periodic groups II-VI, III-V, or IV-IV. The size of QD ranges from several to tens of nanometers (10¡9n) in diameter, which is about 10-100 atoms'. A QD can contain from a single electron to several thousand electrons since the size of the quantum dot is designable. QD are fabricated in semiconductor material in such a way that the free motion of the electrons is trapped in a quasi-zero

dimensional dot. Because of the strong confinement imposed in all three spatial dimensions, a QD behaves similarly to atoms and is often referred to as artificial atoms.A QCA cell as shown in Fig. 1 is considered as a square with four dot as its corners. The cell is loaded with two extra electrons (free electrons), which can quantum mechanically tunnel between cell dots but cannot tunnel between cells. With the placement of these two extra electrons in the four dots and due to the electrostatic repulsion, the two free electrons only can be at two stable positions. These two conditions considered as -1 and +1 polarity or Boolean values 0 and 1 respectively [3]. Fig.2 shows these conditions. As it was maintained, the two free electrons of each cell can only be in two stable conditions. The movement of each cell free electrons between its dots is done through tunneling mechanism. There are some barriers among adjacent dots in each QCA cell (inter-dot barriers) whose control can lead to a control of the free electrons and hence control the polarity of each QCA cell.

Various types of QCA devices can be constructed using different physical cell arrangements [8]. The fundamental QCA logic elements include a QCA wire, QCA inverter, and QCA majority gate .

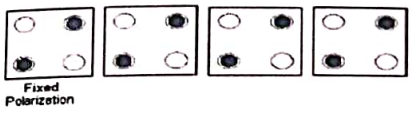


Figure 3 90 QCA Wire

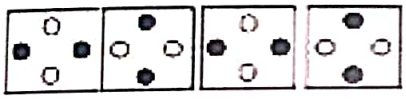


Figure 4 45 QCA Wire

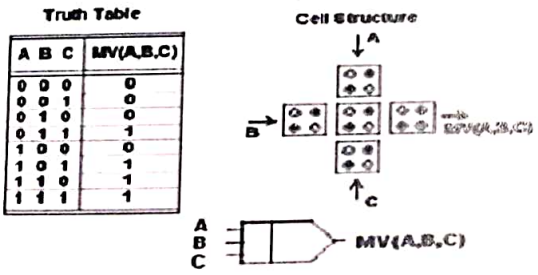


Figure 5 QCA majority Gate

In a QCA wire, the binary signal propagates from input to output because of the electrostatic interactions between cells. The propagation in a 90° QCA wire is shown in Fig. 3. Other than the 90° QCA wire, a 45° QCA wire can also be used. In this case, the propagation of the binary signal alternates between the two polarizations .Other QCA basic element is the majority voter (MV) with logic function MV (A,B,C) = AB + AC + BC. MV can be realized by 5 QCA cells, as shown in Figure 4. Logic AND and OR functions can be implemented from the MV by setting an input permanently to a '0' or '1' value.

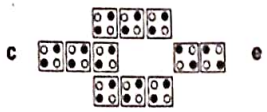


Figure 6 QCA Inverter

The inverter is the other basic gate in QCA and is shown in Figure 6. In inverter, the 45° displacement in the two lines of merging cells, produces complement action of the input signal. By majority voter gates and inverter It is possible to make logic circuits. Various circuits have been designed by QCA technology [10,11,12,13].

A further feature of QCA is the clocking process, clocking of QCA circuits requires a completely different approach than CMOS. A clock provides both synchronization and power gain to the QCA circuit [14]. The QCA clock is implemented by applying an E field that controls the potential barriers between quantum dots. The change in potential barriers allows to control the rate at which the electrons quantum mechanically tunnel between the dots in the QCA cell and therefore, the switching of its polarization. When the clock signal (through the E field) is low, the potential barriers between dots are low because no polarization exists.

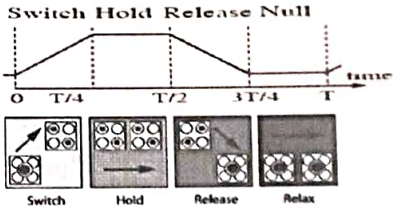


Figure 7 Clocking process in QCA

Clocking in QCA [14] is implemented as follows: the QCA circuit layout is divided in adjacent zones that pertain to the four phases of the clock. Each of the clock signals is shifted by 90 degrees from the previous one as shown in Fig. 7. The slope of the transitions must be sufficiently small to maintain the cells near the ground state. This technique (known as quasi-adiabatic switching) has been proposed in [14]. In the first phase, the clock signal rises (the switch state) and the polarization of the cell is dependent on the neighboring cells. In the second phase (the hold state), the clock signal remains high, thus preventing the tunneling of the electron pair and therefore, latching the information inside the cell. In this phase, the information can be used as input to the neighboring cells that are in the switch state. In the third phase (the release state), the clock signal is lowered and the cell becomes unpolarised. In the last phase (the relax state), the clock signal is kept low and the cell stays unpolarised.

III. QCA MEMORY CIRCUITS OVERVIEW

When transistors are scaled down in size, many problems arise to in memory circuits. First the leakage current increases. Leakage current translates to heat generation which limits the density of storage. If memory cells are too close together, the

heat generated could destabilize the cells. This constraint will limits the density of CMOS memory at the nanoscale. Memory array architecture does not translate well to the nanoscale due to an increase in both transient and permanent errors. Transient faults will be more common because the energies at which bits are stored will be lower than current memories and will therefore be more susceptible to fluctuations due to doping problems both at fabrication time and caused by electro migration of atoms during memory operation. Permanent errors will also be more common because of the difficulty of fabrication at the nanoscale. Memory design in QCA present unique characteristics due to their clocking structure. Since memory is one of the most applicable basic units in digital circuits, having a fast and optimized QCA- based memory cell is remarkable. Various works have been done in the memory architectures based on QCA.

In the technical literature, QCA based memories can be mainly classified into parallel and serial architectures. A parallel architecture offers the advantage of low latency, at each memory cell, only one data bit is stored, so there is no delay in that bit reaching the Read/Write circuitry. In a serial design, multiple bits are stored in each memory cell and share the Read/Write circuitry, thus resulting in a delay proportional to the word size. [15] has made an early attempt to design a serial QCA memory using the so-called **SQUARES formalism.** The basic principle of this technique is to define a set of equally sized blocks, each performing a basic function in QCA. These blocks can then be tiled together to design more complex QCA circuits. The obvious advantage of this technique is the ease in the geometric layout. However, as the blocks are of standard size, a substantial unutilized area appears in each block, thus causing spatial redundancy and lower density in the overall design. Clocking each SQUARE requires a large number of clocking zones even for a modest memory size, thus also requiring a considerable amount of CMOS circuitry to generate the clocking signals. [16] has introduced a **H-Memory architecture** with high density and uniform access time. The H-Memory has a complete binary tree structure with control circuitry at each node; as the memory spirals are at the leaf nodes, an integration of logic and memory is accomplished in the layout, but the control circuitry and memory are logically separate (similarly to CMOS design). However unlike conventional designs, control and data bits are serialized. The bit stream enters the memory structure at the root node and traverses down the tree by utilizing one control bit for routing at every node in the path. The architectural choice of dealing with serial bit streams results also in rather complex control logic for QCA. The memory cell at each leaf node is a spiral allowing storage of several bits, while sharing clocking zones between multiple loops. In this design, the memory size at each spiral and the cell count do not have a linear relationship; each outer loop has an increasing diameter, thus requiring more QCA cells for its implementation (although its storage capacity remains constant). [17] has proposed a **conventional parallel memory architecture** (such as encountered in CMOS-based RAM design) for QCA, i.e. by storing one bit at each memory cell. The single-bit memory cells allow the design of a simple Read/Write circuitry; each memory cell is implemented using 170 QCA cells and the select signals are separately generated using decoders. The main disadvantage of this approach is the same as the one encountered in [15] namely, data in each memory cell is stored using a closed QCA wire loop (which is partitioned into four clocking zones). Also, clocking zones cannot be shared between memory loops and their dimensions are very small. Therefore, the memory design requires a large number of clocking zones, thus complicating the routing of underlying clock lines. The **hybrid memory architecture** [18] combines the advantages of reduced area of a serial memory with the reduced latency in read operation of a parallel memory, hence its name the hybrid. This architecture is best suited in applications in which data is written rarely or in a burst mode, but the read operation is performed often (e.g. like the program memory of a microprocessor).

There are two common type of memory cell in QCA: Loop based memory cell and Line based memory cell. The popular loop based memory cell proposed in [15] stores data bits circulating on the feedback loop (Fig 9) of QCA cells. The feedback is processed within four clocking zones. These four clocking zones are generated by the conventional four phases of clocking strategy, as illustrated in Fig. 10, thus no additional clock generators are necessary. Furthermore, the read/write circuitry can be quite complex for serial access memories. Above mentioned all architecture used the loop based memory cell.

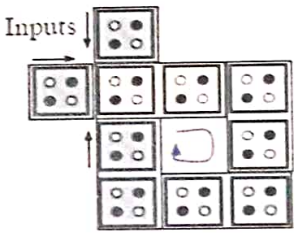


Figure 8 Loop based memory cell

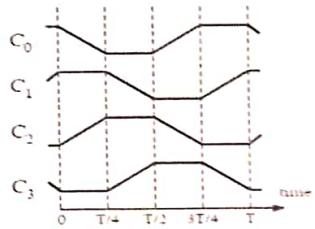


Figure 9 Conventional four phase clocking

The line based memory cell stores data bits propagating back and forward on a line of QCA cells. The **Line Based Memory[19]** is a novel logic arrangement for the MV, namely the wires to an MV can behave differently (either as input or output) in time depending on the clock phase in which they are operative. This arrangement combined with a new clocking strategy, overcomes the limitation of a traditional unidirectional flow of logic signals in QCA.The

line-based memory design in [20] uses three clock zones (in addition to the four clock zones on the rest of the circuit) as shown in Fig.11. [20] purposed the parallel memory architecture using the line based memory cell. This architecture requires two additional clocking signals as the line based operation of the memory cell needs three zones and four step process whose timing is different from the commonly used for adiabatic switching.

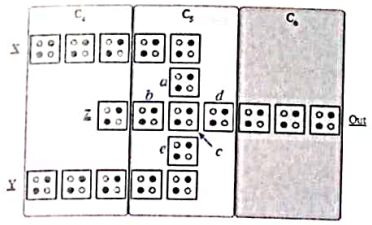


Figure 8 Line based memory cell

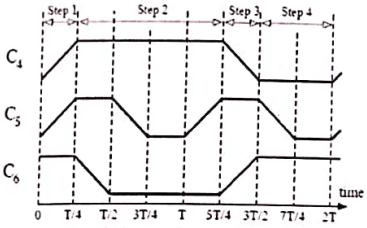


Figure 9 Three phase clocking scheme for the line memory

The line based parallel memory design proposed in [21] requires an easy-to-implement, dual-phase clocking scheme. Dual-phase clocking is implemented with two clock phases which have the same duty cycle and are phase-shifted by half a clock cycle, thus, requiring only one additional clock generator. Hence this reduces the number of QCA cells and clocking zones of the three-phase implementation presented in [20]. A Line based serial memory architecture [22, 23] consists of two long horizontal wires connected together at both ends by two short verticals wire, thus creating a loop for memory in paradigm. Thus in this architecture utilizes new building block (called tiles) in the storage and input output circuitry. Clocking zones are shared between memory cells and length of QCA line of a clocking zone is independent of the word size.

The main advantage of the line-based approach is that the clocking distribution circuitry is dramatically simplified because the same clocking zones can be shared by different memory cells. In brief, compared to the loop-based memory cell, line-based memory cells are much simpler in that line based memory cells can be stacked into a matrix structure. Also, the density of the line-based memory is higher than the loop-based memory cell, as the unused space inside the feedback loop affects utilization.

However,peripheral Read/Write circuits of these architectures [22, 23] are complex, clock circuitries and the entire memory cell are still difficult to fabricate despite the improvement compared to loop-based core. Clock zones do not have a clear and regular partition. Moreover, these two kinds of memory cell cost many cells, control cells and layout areas. Thus the improves memory cell [24] that exploits regular clock zone by employing two new clocking signals and a compact Read/Write circuit. The clock circuitry is very regular, helping manufacturability for physical implementation.

[25] proposed a more efficient memory design around line based memory introducing parallel read. The proposed supporting logic enables realization of such a high speed memory system. Its power to execute simultaneous read write operation is exploited in designing digital signal processors.

[26] purposed improved loop-based Random Access Memory (RAM) cell. In this the inherent capabilities of QCA, such as the programmability of majority gate and the clocking mechanism have been considered. The wasted area has been reduced compared to traditional loop-based RAM cell and the memory access time has been duplicated in presence of smaller number of cells. In [27] memory cell with set/ reset ability will be introduced. This designs have a simple and robust structure and do not need any crossover wire.

IV. CONCLUSION

Nanoelectronics, including quantum-dot cellular automata, focuses on the integration of molecule sized elements. By joining these elements in specific patterns, engineers and scientists have the potential to create a new generation of logic and digital capabilities far beyond what Moore's Law projected for transistors some 30 years ago. There are many challenges to overcome before quantum dots will affect society on a daily basis, including temperature requirements and the feasibility of mass production. Yet, working together in multidisciplinary teams, researchers can and will find a way to make circuits smaller, faster, and better.After review the QCA and QCA Memory Architecture previous work still there are many limitations. The following issues in QCA memory Circuits design:

- Provide a regular and simple clock zone which help manufacturability for physical implementation.
- Provide compact Read/Write signal
- Remove waste area in memory cell.
- Sharing the clock zone.
- Synchronization in memory cell clock and other memory circuits for proper operation.
- Increase in memory capacity.

Nanoscience offers new frontiers in engineering devices on a molecular level that are well on their way to us hering electronics into the next century.

Thus the design of QCA memory cell and memory architecture calls further improvement for getting high density , high speed , less power ,high performance and larger memory word.

REFERENCES

[1] International Technology Roadmap for Semiconductors ,Executive summary, 2011 Edition.

[2] Compano, R., Molenkamp, L., Paul, D.J. 'Technology roadmap for nanoelectroincs', in European Commission IST programme, Future and Emerging Technologies.

[3] C.S. Lent, P.D. Tougaw, W. Porod, and G.H. Bernstein, "Quantum cellular automata," Nanotechnology, vol.4, pp.49–57, 1993

[4] Lent, C.S., Tougaw, P.D., and Porod, W.: 'Quantum cellular automata: the physics of computing with arrays of quantum dot molecules'. PhysComp 94: Proc. Workshop on Physics and Computing, IEEE Computer Society Press, 1994

[5] Lent, C.S., and Tougaw, P.D. 'A device architecture for computing with quantum dots', Proc. IEEE., 85, pp. 541–557,1997

[6] Timler, J., and Lent, C.S.: 'Power gain and dissipation in quantum-dot cellular automata', J. Appl. Phys., 91, pp. 823–831,2002

[7] Islamshah, A., Orlov, A.O., Kummamuru, R.K., Bernstein, G.H., Lent, C.S., Snider, G.L., "Experimental demonstration of a leadless quantum-dot cellular automata cell", Appl. Phys. Lett., 77 (5) 738, 2000

[8] P. Tougaw and C. Lent, Logical devices implemented using quantum cellular automata. Journal of Applied Physics, 75 ,1994.

[9] C.S.Lent and P.D.Tougaw, "Lines of interacting quantum-dot cells: A binary wire", Journal of Applied Physics, vol.74, no.10, pp.6227–6233,November15, 1993.

[10] Cho H, Swartzlander EE. 'Adder designs and analyses for quantum-dot cellular automata'. IEEE Transactions on Nanotechnology , 6(3):374–383,2007.

[11] Graunke CR, Wheeler DI, Tougaw PD, Will JD. 'Implementation of a crossbar network using quantum-dot cellular Automata', IEEE Transactions on Nanotechnology , 4(4):435–440, 2005.

[12] M. Niemier and P. M. Kogge, 'Logic-in wire: Using quantum dots to implement a microprocessor', In International Conf. on Electronics, Circuits, and Systems (ICECS '99), Sept. 1999.

[13] Dimitrov, V.S., Jullien, G.A., and Walus, K., 'Quantum-dot cellular automata carry-look-ahead adder and barrel shifter', IEEE Emerging Telecommunications Technologies Conf., 2002

[14] M. Ni Lent, C.S.and Isaksen, Clocked molecular quantum dot cellular automata, IEEE Trans. Electron Devices, vol. 50, pp. 1890-1896, Sept. 2003.

[15] Berzon, D.; Fountain, T.J. , 'A memory design in QCAs using the SQUARES formalism', In Proc. 9th Great Lakes Symp. VLSI, pp. 168-172, 4-6 Mar 1999.

[16] S. Frost, A. Rodrigues, A. Janiszewski, R. Rausch, and P. Kogge., 'Memory in motion: A study of storage structures in qca. In First Workshop on Non-Silicon Computing, 2002.

[17] Walus K., Vetteth, A., Jullien, G.A., Dimitrov, V.S., 'RAM Design Using Quantum-Dot Cellular Automata', NanoTechnology Conference,vol 2, pp. 160-163, 2003.

[18] Ottavi, M., Pontarelli, S., Vankamamidi, V., and Lombardi, F. 'Design of a QCA memory with parallel read/serial write: design and analysis'. Proc. IEEE Computer Society Ann. Symp. on VLSI, Vol 153, No 3, June 2006,

[19] Marco Ottavi, Vamsi Vankamamidi and Fabrizio Lombardi, 'Novel memory designs for QCA implementation', Proc. 5th IEEE Conf. on Nanotechnology, July 2005

[20] Vankamamidi, V.; Ottavi, M.; Lombardi, F. 'A line-based parallel memory for QCA implementation', IEEE Trans. on Nanotechnology , vol.4, no.6, pp. 690- 698, Nov. 2005

[21] Baris Taskin, Bo Hong, 'Improving line-based QCA memory cell design through dual phase clocking', IEEE Trans. on VLSI 16, pp 1648–1656,2008

[22] Vankamamidi V, Ottavi M, Lombardi F., 'A serial memory by quantum-dot cellular automata (QCA)', IEEE Trans. on Computers , 57(8):606–618, 2008

[23] Vankamamidi, V.; Ottavi, M.; Lombardi, 'Tile-based design of a serial memory in QCA', In Proc. 15th ACM Great Lakes symp. on VLSI (GLSVLSI '05), 2005

[24] Xiaokuo Yang, Li Cai, Hongtu Huang and Xiaohui Zhao , 'A comparative analysis and design of quantum-dot cellular automata memory cell architecture', Int. J. Circ. Theor. Appl. (Wiley),40:93–103, 2012

[25] Bibhash Sen, Anshu S Anand, BipJab K Sikdar, ' Efficient Design Of Memory Based On Quantum-Dot Cellular Automata', In IEEE conf. (TENCON 2011), pp. 768 – 772, 21- 24 Nov 2011.

[26] Mostafa Abdollahian Dehkordi, Abbas Shahini Shamsabadi, Behrouz Shahgholi Ghahfarokhi, Abbas Vafaei ,Novel RAM cell designs based on inherent capabilities of quantum-dot cellular automata, Microelectronics Journal (Elsevier) 42, 701–708,2011

[27] Sara Hashemi , KeivanNavi , 'New robust QCA D flip flop and memory structures', Microelectronics Journal(Elsevier) ,vol. 43 ,pp 929–940, 2012

KIET IJCE KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

An Intelligent Opinion Mining for Customer Reviews

Minal M.Thawakar[1], Prof.Sheikh Phiroj[2]
Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, India

Abstract- **Today opinion mining is fast growing topic as more and more people use internet in their day to day life and share information globally. Due to increase in social networking and micro-blogging people share their views, opinion and emotions with each other. This information is necessary for the organization that are selling or manufacturing products in order make changes in design and other configuration of the product. As number of customers give their reviews on same product so that it is difficult for the new user to take decision whether to buy a product or not. The proposed system gives an enhanced summarized result for newly users in order to take fast decision. It extends the level of feature based opinion classification. A soft computing technique is used to classify opinion into positive and negative opinion. The result is shown in textual as well as in graphical form. It not only gives the summary of individual model of a car but also compare two models of a car. By using proposed system, it is easy for user to learn the characteristics of a model as well as to take decision.**

Keywords: **Opinion mining, feature extraction, soft computing, ruled based fuzzy logic, opinion classification, summarization.**

I. INTRODUCTION

World Wide Web contain huge amount of information which consist of online opinion such as political affair comments, news comments, product comments etc. Internet users express their personal views on review websites, blogs, and discussion forum and so on. This information is publically available to users through internet. However large amount of opinion on the Web makes it difficult to get important information. Reading all reviews is a time consuming and confusing task. The research has been going on mining customer reviews which is called as opinion mining.

Opinion mining is the field of study people's emotions, views, experiences from written language. It is the field of natural language processing, data mining, machine learning, and artificial intelligence and so on. The interest in opinion mining has been increased due to increase in social media services such as review sites, micro-blogs, online social network etc. Today online opinion is very beneficial for businessman for collection of feedback from customers so that necessary changes can be made with product. Opinion mining is not only useful for consumer but also for producer.

In this research, we propose a feature based opinion summarization on customer reviews of automobiles. The task is performed in following steps:

1. Identify the features of automobiles that customer have commented.
2. Show all reviews of automobile according to selected features.
3. Now according to selected feature divide reviews into positive and negative reviews.
4. Show overall summary of reviews using graph which consist of histogram of positive and negative review according to features.
5. According to features show individual graphical summary of positive and negative reviews.
6. Finally comparison is made between two models and show graphical summary

We give a simple example to demonstrate the above steps. Consider the review of automobile having company and model as Maruti Suzuki and Alto K10 respectively.

Company: Maruti Suzuki
Model: Alto K10
Review all:
Look and style:
<individual comments>
< individual comments>
< individual comments>

Comfort:
<individual comments>
< individual comments>
< individual comments>

Positive reviews:
Look and style:
<individual comments>
< individual comments>

< individual comments>

Comfort:
<individual comments>
< individual comments>
< individual comments>

Negative reviews:
Look and style:
<individual comments>
< individual comments>
< individual comments>

Comfort:
<individual comments>
< individual comments>
< individual comments>

For the above example review all consist of all reviews that is the combination of positive and negative reviews and positive and negative reviews contains positive opinion reviews and negative opinion reviews from review all respectively.

Our task is different from others in number of ways. We textually as well as graphically represent the summary of reviews. We mainly focused on features of automobiles that customers have opinion and also whether the opinion is positive or negative according to features.

A soft computing technique is used to perform classification of opinion into positive and negative opinion. Here soft computing technique called rule-based fuzzy logic is used where fuzzy function is used to calculate the score of the sentence.

Section 2 describes related work on feature mining. Section 3 contains detail working of proposed system. Section 4 describes the experimental results. Finally we give conclude and give direction for future work in opinion mining field.

II. RELATED WORK

The following section explains the survey of various papers based on feature based opinion mining. Several methods have been proposed to extract feature from customer reviews.

Hu and Liu [3] worked on customer reviews. They extract features of product from customer reviews. They also show whether the opinion is positive or negative and finally summarize the result. The main problem with the method employed by this system is it does not give proper relation between feature and its opinion. In our work we not only decide whether the opinion is positive or negative but also calculate the score of the word which is used for the plotting graph.

Lawrence and David [4] developed an automatic method which distinguishes positive and negative reviews. Aciar [5] proposed a feature extraction method based on ontology. But the main problem with this is, whenever new feature is added there is a need of construction and updating of ontology each time. Hana Jeong, Dongwook Shin, and Joongmin Choi [11] developed an enhanced feature extraction technique called FEROM which effectively extract correct feature from the review data but the main problem with this method it does not calculate the strength of the opinion and does not give proper summarize form. But in our approach we not only calculate the strength of the opinion but also give a detailed summary of each model according to selected features

Various machine learning methods and training sets are used to perform automatic text classification. Machine learning methods such [13] as Support Vector machine (SVM), Artificial intelligence [14], Naïve Bayesian [12] or hybrid approaches [15, 16] are used to improve the efficiency of classification. But all these methods are not focused on generating extractive summaries.

III. PROPOSED TECHNIQUE

The following section describes the design of our proposed feature based opinion mining system based on rule-based fuzzy logic. Our proposed opinion systems automatically extract the opinion from unstructured user reviews and classify the opinion into positive and negative opinion according to the assigned polarity. Polarity is a sometime considered as intensity. The proposed systems consist of following steps: 1) Data Preprocessing 2) Feature and opinion generation 3) Opinion Classification 4) Summary.

We perform opinion mining on online reviews of various car models. Reviews are collected from different automobiles websites having engine capacity between 800-1000 cc. The websites that we are using for collection of reviews are www.carwale.com and www.cardekho.com. We collect approximately 450 reviews for 9 car models where each model having approximately 50 reviews.

Figure 1 shows the system architecture. The different steps of the system architecture are explained below.

A) Data Preprocessing: User's opinions are generally expressed in natural language which contains errors in spelling, grammar, mistakes in punctuations and so on. Before mining user-

generated reviews need preprocessing in order to remove noise. An openNLP tool is used to perform this task. openNLP tool is a machine learning natural language processing tool used to perform following task such as sentence detection, tokenization, POS tagging, chunking, parsing. The version of openNLP tool use is 1.5.3. openNLP tool consist Standford parser which is a well known linguistic parser. It automatically corrects the unstructured text and produces a clean text.

Consider an example; a user-generated review is in the form of

"the look and style of a car is so nice!!!"

After preprocessing the sentence would read as,

"The look and style of a car is so nice!"

In the above example, the first sentence is capitalized and the repetitive exclamation mark occurs only once.

Thus the preprocessing step generates a clean text which is given as input to the next step of the system.

B) Feature and Opinion generation: In this step we generate a feature set for opinion mining from cleaned reviews generated in first step by using linguistic parser. Here we have created a table name as Feature and Opinion generation table (FOGT). FOGT table consist of car model features as well as positive, negative and inverter words associated with that feature. We manually assign weight to each word in the table. We use a standard WordNet directory for making FOGT table. Table 1. Shows the entries in FOGT. Here POS (part-of-speech) tagging is used to performed feature extraction. Frequently occur Noun (N) and Noun Phrase (NP) is considered as feature and Adjective or Adverb is considered as opinion word for the sentence.

For example, consider a review of sentence for model of a car creates after preprocessing is:

"The look of car is nice."

When POS tagging is done by using openNLP the output is generated as:

"The look [.n] of [.p] car [.n] is [.v] nice [.a]"

In the above example, [.n] denotes noun, [.p] denotes preposition, [.a] denotes adjective and [.v] denotes verb. Here "look" is considered as feature which is described by adjective "good". Adjective "good" shows the opinion about feature "look". Whenever POS tagging is done noun, noun phrases, adjective or adverb of the sentence is checked with the entries in the FOGT.

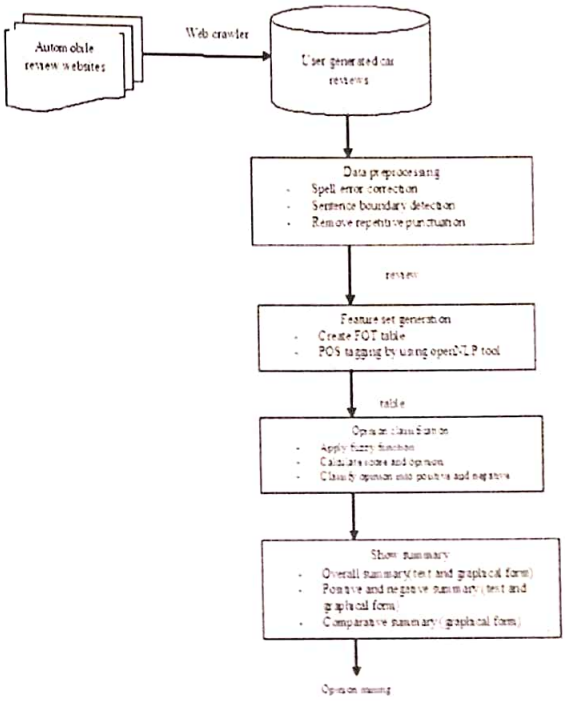


Figure 1. System architecture

Feature	Positive polarity words (p=1)	Negative polarity words (p=-1)	Inverter
Look and style	Excellent, good, best, decent, attractive, great, beautiful, elegant, amazing, stylish	Worst, bad, poor	Not, Never
Comfort	Comfortable, extraordinary	congested	Not
Mileage	Decent, satisfactory, reliable		Not
Pickup	Average, sufficient, high, fine	Slow, less	
Overall experience	Happy	Mistake, down, cheat, waste	
Fuel economy	Superb, fantastic	Low	Not

Table 1. Feature and Opinion Generation Table

Consider the first entry in the FOGT, it indicate the feature "look and style" for a car model. This feature can take fuzzy values like "excellent", "good", "best", "decent", "attractive", "great", "beautiful", "elegant", "amazing" and "stylish" which has positive polarity. On the other hand it can take fuzzy values like "worst", "bad" and "poor" which have negative polarity. The polarity of words is reversed by inverter which has words like "not" and "never."

The FOGT table is used in next step to calculate the score of the user review sentence and classify it into positive and negative review.

C) Opinion Classification: In this step, the reviews are classified into positive and negative reviews. We classify new user review by calculating fuzzy score. The fuzzy score is calculated by using following steps. 1) Extract feature and words from FOGT look up table. 2) Identify the polarity and initial weight of the word. 3) Calculate overall score using fuzzy function. The first two steps of fuzzy score calculation are explained in above second step of system architecture. The fuzzy score of the word can be calculated as:

$$f(x) = 1-(1-w(x)) \quad (1)$$

Where $f(x)$ represents fuzzy score of the word and $w(x)$ represents the initial weight of the word which s assigned in FOGT table. Consider $\forall x, (x) \in [0, 1]$ which indicate the output value of $f(x)$ should be in the range of [0, 1]. For example, the initial assigned weight of the word "good" is 0.5, hence fuzzy score for the particular word is calculated as $f(x) = 0.5$. The FOGT table contains polarity for identification of positive and negative opinion. Hence the modified fuzzy score can be calculated as:

$$f(x)_{new} = p_i f(x) \quad (3)$$

In the above equation, the first term indicate the polarity of the feature. If polarity is positive then the value of $p_i = 1$ otherwise the value of $pi = -1$. If inverter is present (ex. "not") then simply reverse the value of polarity which is indicated by '*pi*'. The inverter only changes the polarity of the feature but the magnitude remains unchanged. Equation (3) is used to plot overall graph. The value of $f(x)_{new}$ calculated using (3) remains in the range of [-1,1] so we need to normalized the value of $f(x)_{new}$ .The normalized value should be in the range of [0,1], It is calculated in the following manner:

$$f_n(x) = \frac{f(x)new + 1}{2} \quad (4)$$

The normalized value is generally used to plot positive/negative graph. The accuracy of this classification is verified by comparing them. Comparison is made on the basis of features of two different models of car.

D) Summary: This is the last step of system architecture. Here we have generated a detailed summary of reviews according to selected features in textual as well as in graphical format. It consists of three types of graphs. 1) Overall graph. 2) Positive/Negative graph and 3) Comparison Graph. Figure 1, figure 2 and figure 3 show the graphical summary of reviews for car model Alto-K10.

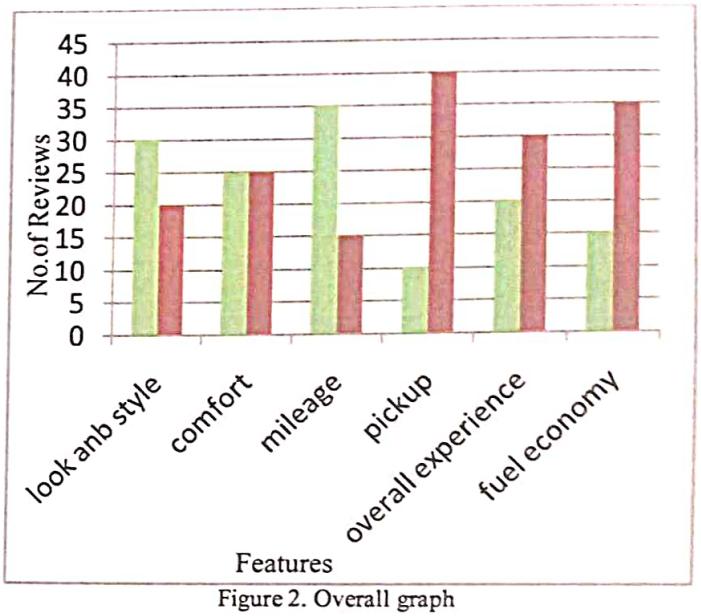


Figure 2. Overall graph

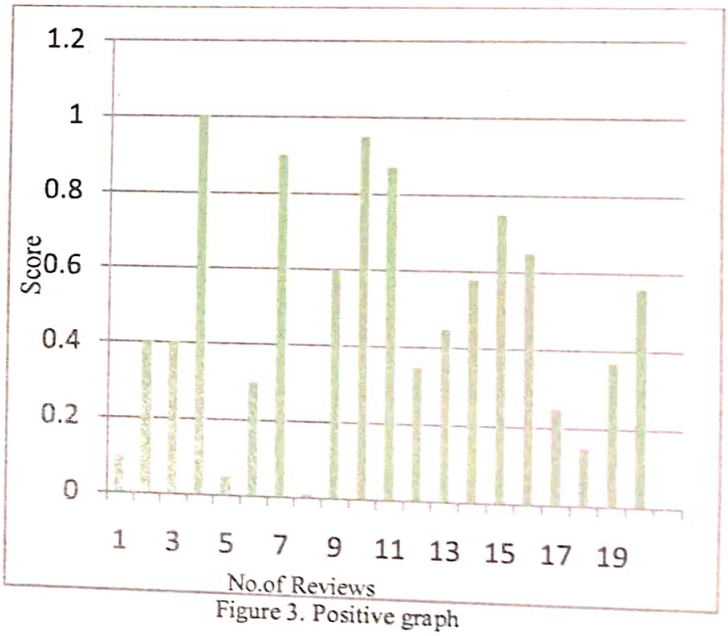


Figure 3. Positive graph

The overall graph contains total number of positive and negative reviews according to selected features. We have taken 50 reviews for each model. Consider for feature overall experience there are 20 positive reviews and 30 negative reviews so the overall graph contain 20 positive and 30 reviews for feature overall experience.

Positive and negative graph contain individual positive and negative reviews according to the score calculated by using equation (4). Overall graph and Positive/ Negative graph is used for verifying individual car model and comparison graph is used for verifying two different models of car.

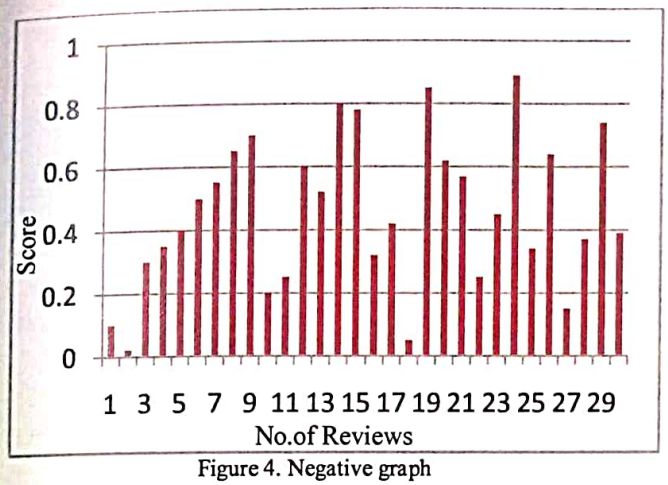


Figure 4. Negative graph

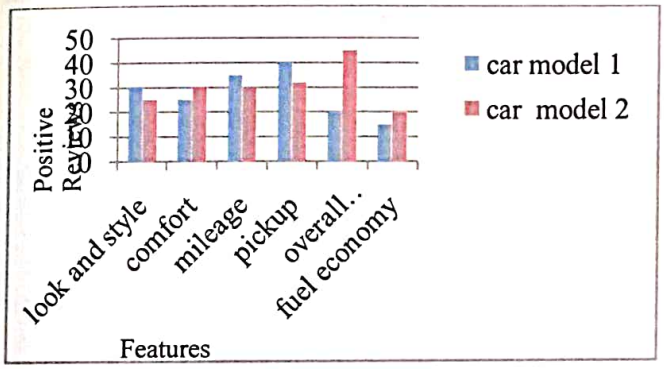


Figure 5.Positive Review Comparison graph

IV. EXPERIMENT RESULTS

This section describes the result of evaluation of our opinion mining strategy. We have conducted the experiment on customer reviews of four different car companies which consist of total nine models. The websites from where we collected the reviews are carwale.com cardekho.com. For each model we first loaded 50 reviews for each model. These reviews were cleaned by using linguistic parser. Feature extraction and opinion word were found by using FOGT table and fuzzy logic respectively. Figure 6. represents the evaluation result. Here customer can get detail summary about car model by selecting company, model and features

V. CONCLUSION

In this paper, we propose a framework for automobiles review extraction based on features. Our experimental results indicate that the proposed technique is very promising in performing the task of opinion mining. We not only predict the positivity and negativity of opinion word, but also calculate the score. The summary is not only useful to common customers, but also for product manufactures.

The primary area of future work is to improve the method of calculate the score/strength of words and use our summarization system end to end in practice

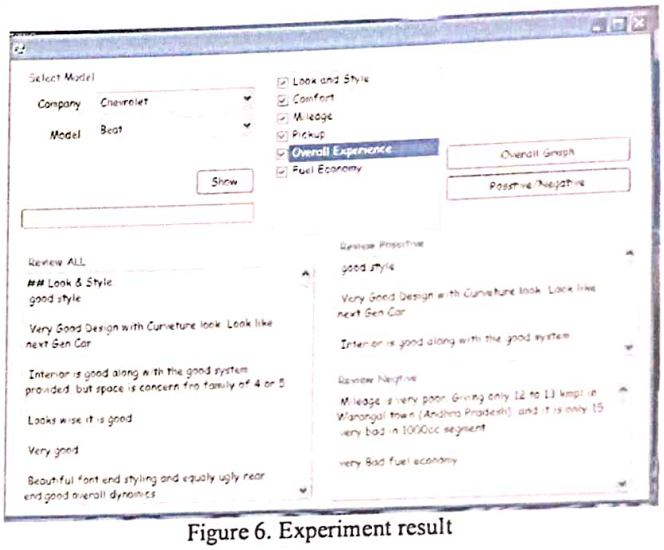


Figure 6. Experiment result

VI. REFERENCES

[1] LiZhen Liu, WenTao Wang, HangShi Wang. Summarizing Customer Reviews Based On Product Features. 2012 5th International Congress on Image and Signal Processing (CISP 2012)

[2] Bing Liu. Sentiment Analysis and Opinion Mining. Synthesis Lectures on Human Language Technologies. Morgan & Claypool Publishers, 2012.

[3] Mingqing Hu and Bing Liu. Mining and Summarizing Customer Reviews. KDD'04, August 22-25,2004, Seattle, Washington, USA.

[4] David M.Blei, Andrew Y.NG and Michael I.Jordan. 2003. Latent Dirichlet allocation. Journal of Machine Learning Research,3(5):993-1022.

[5] S.Aciar et al., "Information Recommender:Basing Recommendations on Consumer Product Reviews," *IEEE Intell. Syst.* Vol. 53, no.9, 2001, pp.1375-1388.

[6]. Hana Jeong, Dongwook Shin, and Joongmin Choi. FEROM:Feature Extration and Refinement for Opinion Mining. ETRI Journal, Volume 33, Number 5, October 2011.

[7] Nikolay Archak, Anindya Ghose, and Panagiotis G. Ipeirotis. Show me the money!: deriving the pricing power of product features by mining consumer reviews. In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '07, pages 56–65, New York, NY, USA, 2007. ACM.

[8] Stefano Baccianella, Andrea Esuli, and Fabrizio Sebastiani. Multi-facet rating of product reviews. In Proceedings of the 31th European Conference on IR Research on Advances in Information Retrieval, ECIR '09, pages 461–472, Berlin, Heidelberg, 2009. Springer-Verlag

[9] Wei Jin, Hung Hay Ho, and Rohini K. Srihari. Opinionminer: a novel machine learning system for web opinion mining and extraction. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '09, pages 1195–1204, New York, NY, USA, 2009. ACM.

[10] Fangtao Li, Minlie Huang, and Xiaoyan Zhu. Sentiment analysis with global topics and local dependency. In Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence (AAAI), 2010.

[11] Hana Jeong, Dongwook Shin, and Joongmin Choi. FEROM:Feature Extration and Refinement for Opinion Mining. ETRI Journal, Volume 33, Number 5, October 2011.
[12] S. Kim, K. Han, H. Rim, and S. H. Myaeng, "Some effective techniques for na¨ıve bayes text classification," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 11, pp. 1457–1466, 2006.
[13] Z.-Q. Wang, X. Sun, D.-X. Zhang, and X. Li, "An optimal SVM-based text classification algorithm," in *Proceedings of the International Conference on Machine Learning and Cybernetics*, pp. 1378–1381, August 2006.
[14] Z. Wang, Y. He, and M. Jiang, "A comparison among three neural networks for text classification," in *Proceedings of the 8th International Conference on Signal Processing (ICSP '06)*, pp. 1883–1886, November 2006.
[15] D. Isa, L. H. Lee, V. P. Kallimani, and R. Rajkumar, "Text document preprocessing with the bayes formula for classification using the support vector machine," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 9, pp. 1264–1272, 2008.
[16] R. D. Goyal, "Knowledge based neural network for text classification," in *Proceedings of the IEEE International Conference on Granular Computing (GrC '07)*, pp. 542–547, November 2007.
[17] S. Shi and Y. Wang, "A product features mining method based on association rules and the degree of property co-occurrence," in *Proceedings of the International Conference on Computer Science and Network Technology (ICCSNT '11)*, vol. 2, pp. 1190–1194, December 2011.
[18] LiZhen Liu, WenTao Wang, HangShi Wang, "Summarizing Customer Reviews Based On Product Features" 2012 5th International Congress on Image and Signal Processing (CISP 2012)
[19] Mohammad Khabbaz, Keivan Kianmehr, and Reda Alhajj "Employing Structural and Textual Feature Extraction for Semistructured Document Classification" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS PART C: APPLICATIONS AND REVIEWS, VOL. 42, NO. 6, NOVEMBER 2012
[20] C. Caragea, A. Silvescu, S. Kataria, D. Caragea, and P. Mitra. "Classifying Scientific Publications Using Abstract Features." In: SARA, Parador de Cardona, Spain, 2011
[21] A. Esuli and F. Sebastiani. 2006. Sentiwordnet: A publicly available lexical resource for opinion mining. In Proc. of LREC 2006.
[22] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment Classification Using Machine Learning Techniques," Proc. EMNLP, Philadelphia, Jul. 2002, pp.79-86.
[23] Minqing H., Bing L. *Mining Opinion Features in Customer Reviews. In Proceedings of AAAI'04* Proceedings of the 19th national conference on Artificial intelligence Pages 755-760.
[24]Mita k. Dalal and Mukesh A. Zaveri, "Opinion Mining from Online User Reviews Using Fuzzy Linguistic Hedges", Applied Computational Intelligence and Soft Computing Volume 2014, Article ID 735942, 9 pages

KIET IJCE KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July – Oct 2014, ISSN: 2320 – 8996

ASIC Design & Implementation of optimized Low Power RC5 Block Cipher

Lomash Chandra Acharya[1], Mr. Dinesh Chand Gupta[2], Dr. Debashis Dutta[3]
Student, Poornima College of Engineering, Jaipur[1]
Assistant Professor, Poornima College of Engineering, Jaipur[2]
Scientist, Department of Electronics and information Engineering, New Delhi[3]
technology.science@gmail.com

ABSTRACT

Today more and more sensitive data is stored digitally. Bank accounts, medical records and personal emails are some categories that data must be kept secured. In modern days consumer electronics wireless communications is a one of the fastest growing sector. The specified security layer of wireless communication protocols provides high level strength. The security layers of these wireless protocols require encryption algorithms to provide transmission security. For this reason designing low power RC5 block cipher has emerges as one of the valuable requirements in portable and wireless applications. RC5 block cipher is based on RC5 encryption algorithm. In this paper, ASIC design and implementation of optimized low power RC5 block cipher has been proposed considering the various aspects such as speed, area and power consumption. Various optimization techniques such as pipelining, resource-sharing and loop wrapping are employed to optimize the design. The parameter of RC5 Encryption algorithm taken are word (w) = 32, round (r) = 4 and key (k) = 128. The simulation is done on Aldec Active HDL. For ASIC Design synthesis is done on Cadence RTL Compiler and physical design is done on Cadence SOC Encounter. ASIC Design ensures very high throughput for RC5 Block Cipher.

Keywords: *RC5 Encryption algorithm, pipelining, resource sharing, loop wrapping, Aldec Active HDL, Cadence RTL Compiler, Cadence SOC Encounter*

I. INTRODUCTION

Cryptography describes a process of encrypting information its meaning is hidden from those user who are not authorized to decrypt the information [1]. Cryptography is used as one of the basic counter measures against system attacks. The cryptography is basically used provide to communication between two people to communicate over a communication channel in such a way that an unauthorized person cannot understand what is being communicated. Data confidentiality, authentication, non-repetition and data integrity are some of the main parts of cryptography. A cryptographic algorithm is also called as a cipher or a block cipher is a sequential process of mathematical operations used to encrypt and decrypt information [2]. There are basically two process of a cryptographic algorithm: (i) Encryption (ii) Decryption

Encryption is a process of encoding input data in such a way that only authorized user can read the data. Encryption does not prevent the hacking of data but it reduces the likelihood that opponent will be able to read the data that is encrypted. Decryption is just a reverse operation of encryption in which encrypted data will be decrypted by authorized user.

II. BACKGROUND

RC5 block cipher is designed by Ronald Rivest in 1994.RC stands for "Rivest Cipher". It is also known as "Ron's Code"[3].It is based on RC5 encryption algorithm. RC5 block cipher is a symmetric block cipher which means same cryptographic key will be used for both encryption and decryption [4]. RC5 encryption algorithm is suitable for both software & hardware implementation. A novel feature of RC5 encryption algorithm is the very heavy use of data-dependent rotations. Due to variable parameter this algorithm is adoptable to different word length processor. The parameter of RC5 encryption algorithm is chosen according to requirement of a particular application. RC5 is a family of encryption algorithms determined by three parameters, as follows [5]:

Table 1: Parameters of RC5 Encryption algorithm

Parameter	Definition	Acceptable values
w	Word size in bits.RC5 Encrypts 2-word blocks.	16,32,64.
r	Number of rounds	0,1,2.....255
b	Number of 8-bit bytes in the secret key K	0,1.....255

A. Basic RC5 Block Cipher architecture

In RC5 block cipher there are basically three routines: key expansion, encryption, and decryption [5, 6]. The key-expansion routine expands user secret key K to fill a key table whose size depends on the selected value of r. Then both encryption and decryption routine uses this same key table. There are basically three types of primitive operations in an encryption routine: modulo addition, bitwise XOR and variable cyclic rotation. The anomalous simplicity of RC5 encryption algorithm makes it easy to implement and analyze. The massive use of data-dependent cyclic rotations is responsible for high level of security of RC5 block cipher. The different types of cryptographic analysis are carried out with the help of data-dependent rotations.

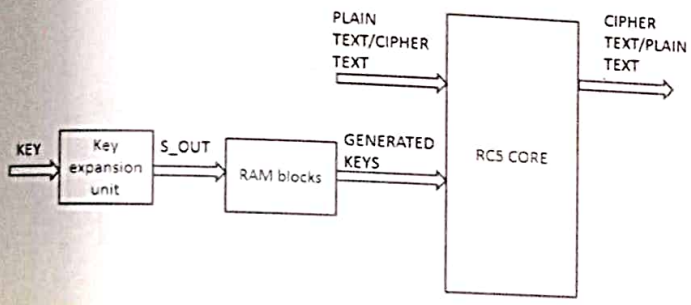


Figure 1: The main units of RC5 crypto system

B. Key expanding algorithm

The key expansion routine expands the user input secret key K to fill the sub key generation array S so that S constitutes an array of length t = 2(r +1) words to get sub keys from S[0] to S[t-1][5, 6]. The two magic constants are used in key expansion algorithm. It is consists of three simple algorithmic parts. The value of two magic constants is as follow:

$$P_w = \text{Odd}((e-2)2^w) \quad \text{---------- (1)}$$
$$Q_w = \text{Odd}((\quad -2)2^w) \quad \text{---------- (2)}$$

Where

e = 2.718281828459..... (Base of natural logarithms)

..... (Golden ratio)

Step 1: Copy the K [0....b-1] into an array L [0....c-1] of c= [b/u] words, where u=w/8 is the number of bytes/word. The pseudo code that achieves the same effect with the assumption that all bytes are unsigned and that array L is initially zeroed.

For i=b-1 down to 0 do

L[i/u]= (L[i/u]<<<8)+K[i]

Step 2: Initialize S to a particular fixed pseudo-random bit pattern, using magic constants Pw and Qw.

The pseudo code for this is given below

S[0]=Pw;

For i=1 to t-1 do

S[i]=S[i-1]+Qw

Step 3: Mix K in three passes over the S and L. Since there is a potentially difference in the sizes of S and L, the larger array will be processed three times and the smaller array may be processed more numbers of times.

The pseudo code for this is given below

i=j=0;

A=B=0;

do 3*max(t, c) times:

A = S[i] = (S[i] +A+B) <<<3;

B = L[j] = (L[j] +A+B) <<< (A+B);

i = (i+1) mod (t);

j= (j+1) mod(c);

Where i and j are counters, A and B are temporary registers.

C. Encryption Algorithm

Input to encryption block is 2w length plaintext stored in two registers A and B, output of this block is 2w length ciphertext. Below figure shows the encryption operation

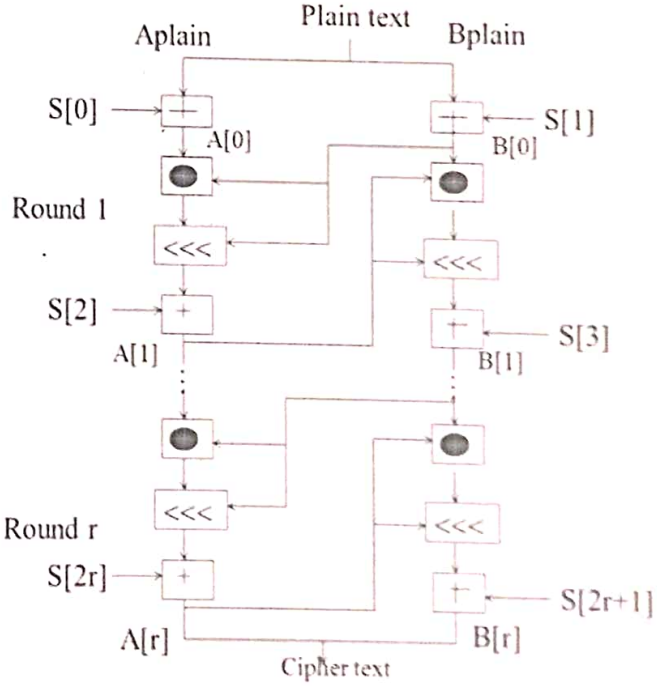


Figure 2: Encryption operation

The pseudo-code for encryption is given as [4, 5]

A =A + S[0];
B = B + S[1] ;

For i = 1 to r do
A = ((A xor B) << B) + S[2 * i] ;
B = ((B xor A) << A) + S[2*i] ;

D. Decryption Algorithm

Input to decryption block is 2w length ciphertext stored in two registers A and B, output of this block is 2w length plaintext. Below figure shows the decryption operation:

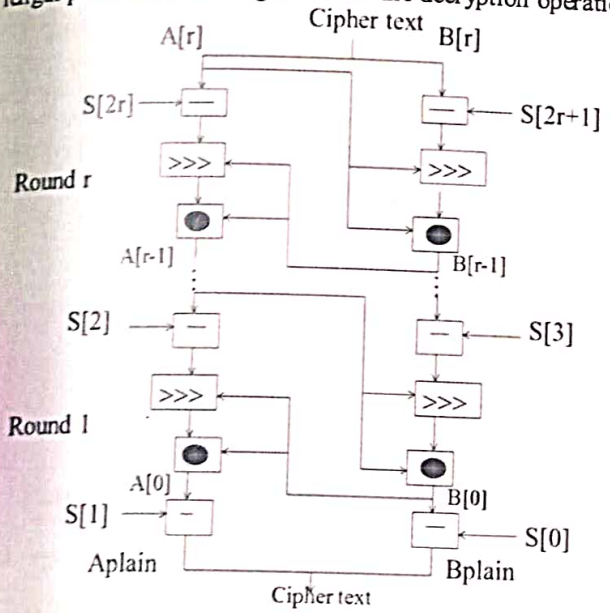


Figure 3: Decryption operation

The pseudo-code for decryption is given as [5, 6]
For i = r down to 1:
B = ((B – S[2i + 1]) >>> A) ⊕ A ;
A = ((A – S[2i]) >>> B) ⊕ B ;
B = B – S[1] ;
A = A – S[0];

E. Basic Operations & their Notations in RC5 block cipher

There are three basic operations (and their inverses) with their notations are used in RC5 block cipher [7].

- The modulo-2^w addition is the sum of words in two's complemented form, denoted by "+".The modulo- 2^w subtraction is it's inverse operation, denoted "-".
- Bit-wise exclusive –OR of words, denoted by ⊗ .
- A left-rotation of words: the left cyclic rotation of word x by y bits is denoted x<<<y. While the inverse operation is right cyclic rotation, denoted by x>>>y.

Most of the modern day processor supports these operations. The rotation operators are only nonlinear operators in RC5 block cipher. The cryptographic properties of data-dependent rotations are responsible for the strength of RC5 encryption algorithm.

III PROPOSED OPTIMIZATION TECHNIQUES

In VLSI Design, a designer has total control on hardware. Because of this optimization of design with respect to area, speed and power takes prime importance. In this paper following techniques are proposed to optimize the design with respect to area, speed and power:

A. Pipelining

Pipelining is a process of increasing resource utilization and to increase the throughput of a design [8]. This technique is commonly used to increase the speed of operation of datapaths in digital processors. For RC5 block cipher pipelining technique is applied to both encryption and decryption operation.

For pipelined implementation of encryption output of one round is stored in one intermediate register and output of this register works as input to the next round. Input to encryption block is 2w length plaintext stored in two registers A and B, output of this block is 2w length cipher text.

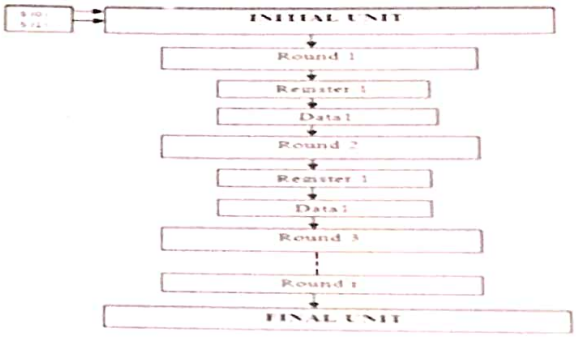


Figure 4: Pipelined Encryption

Decryption is just the reverse operation of the encryption. For pipelined implementation of decryption output of one round is stored in one intermediate register and output of this register works as input to the next round. Input to decryption block is 2w length cipher text stored in two registers A and B, output of this block is 2w length plaintext.

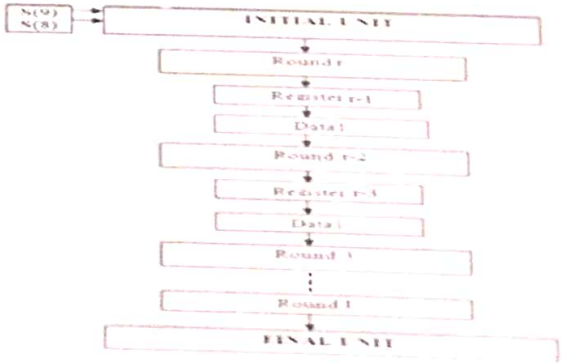


Figure 5: Pipelined Decryption

B. Resource-sharing

If in a two different parts of design are operated at different time and they uses same input resources then resource-sharing is a good choice to save the resources which in turn reduces total area of a design. In this proposed design a common module is used for both encryption and decryption block. This increases hardware efficiency of the design [9].

Since structural modeling is used in Verilog HDL which instantiate encryption or decryption module according to encrypt pin. If encryption pin is high encryption module is called and when encrypt pin is low decryption is called using same registers in design.

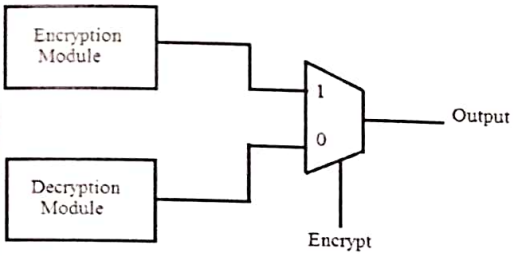


Figure 6: Resource-sharing implementation for RC5 Block Cipher

C. Loop wrapping

In digital circuit design, critical path is path that may cause setup or hold violation. In the proposed design, critical path exists between key input and output of sub key generation stage. This critical path also decides clock period of a design. So it will be fruitful to divide sub key generation stage in more than one clock cycle. This sub key generation stage is used only once when new user secret key is applied.

In Verilog HDL for proposed design, for loop is used for sub key generation stage which runs 30 times for value of r=4.Without application of clock this sub key generation module is designed as a cascading of set of identical modules. This for loop can be wrapped into single module with clock signal and enable input. This enable input remains high over required number of clock cycles till the sub key generation stage is completed. With this technique there is significant reduction in area of the design.

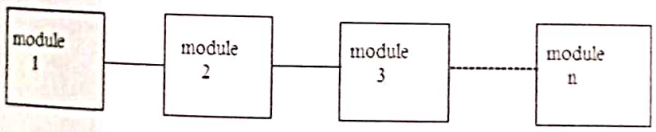


Figure 7: Cascading of identical modules

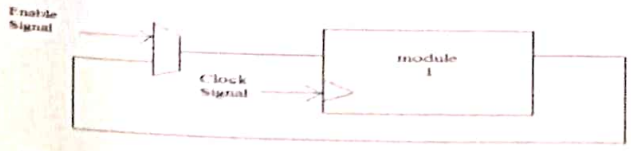


Figure 8: Wrapping of n module into single module

IV. SIMULATION & IMPLEMENTATION RESULTS

The simulation is done using Aldec Active HDL. For ASIC Design synthesis is done on Cadence RTL Compiler using Faraday's 180 nm technology library file and physical design is carried out on Cadence SOC Encounter. The plain text is given as input of encryption core and cipher text is obtained. This cipher text is given as input of decryption core and plain text is obtained. RTL schematic of various modules from Cadence RTL Compiler is given below:

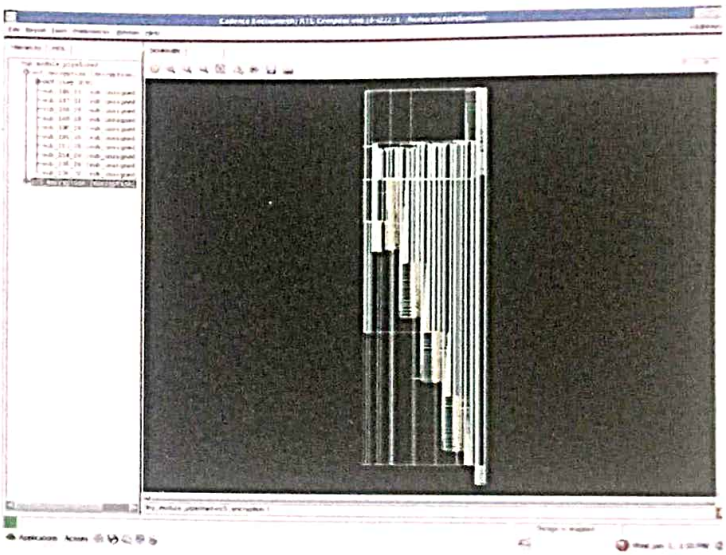


Figure 9: RTL View of Encryption operation

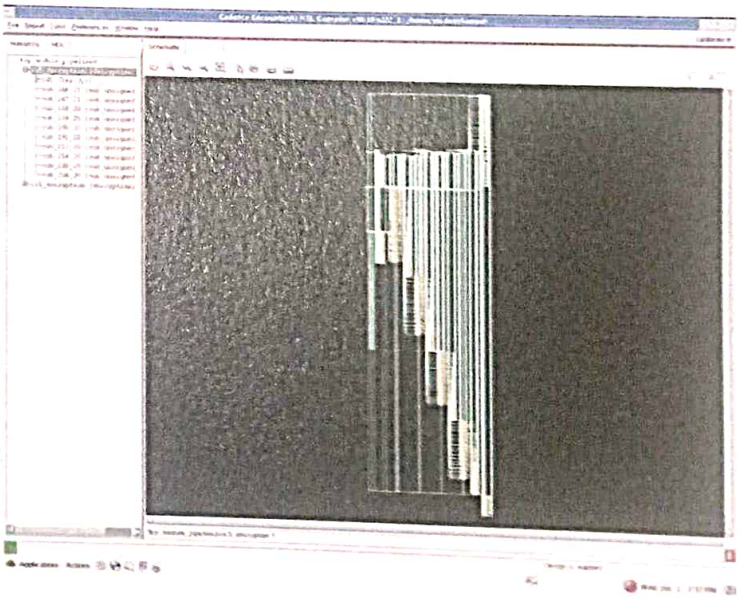


Figure 10: RTL View of Decryption operation

For RC5 Block Cipher without pipelined architecture output is obtained after 2 clock cycles and with pipelined architecture output is obtained after 8 clock cycles. Thus latency is introduced with the application of pipelining but throughput is increase by quite a large margin which is the essential requirement.

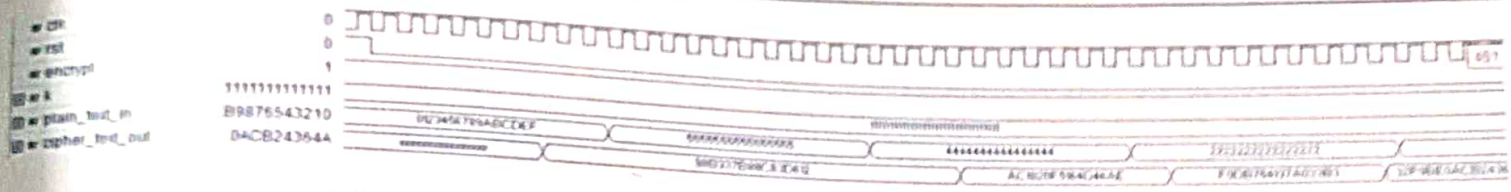


Figure 11: Optimized RC5 Block Cipher Encryption Operation

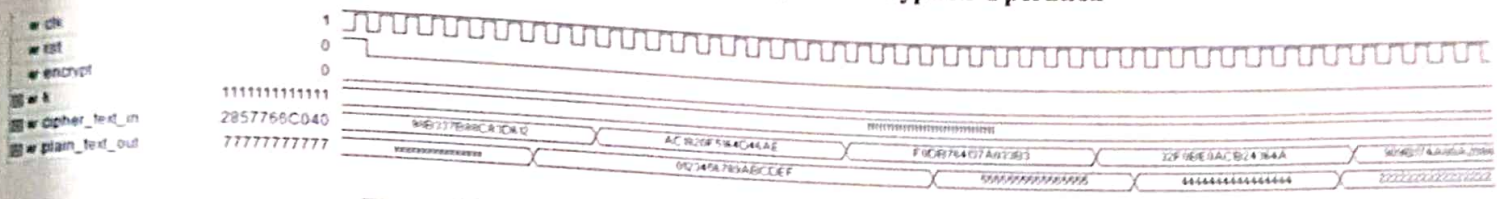


Figure 12: Optimized RC5 Block Cipher Decryption Operation

The physical design results from Cadence SOC Encounter are given below:

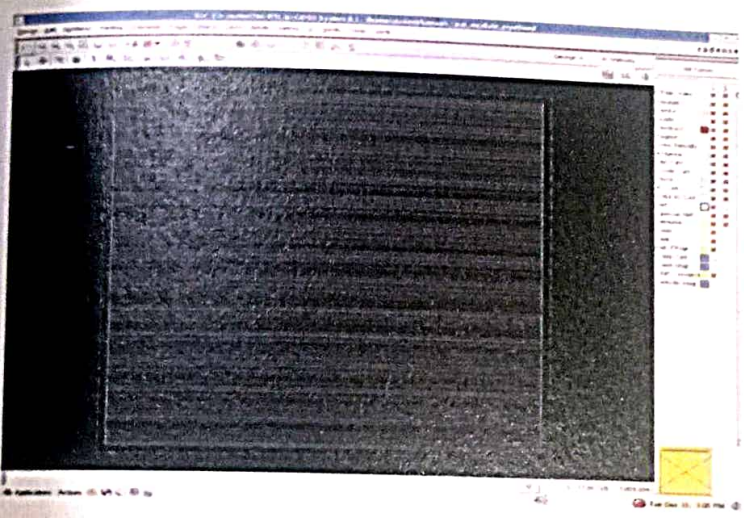


Figure 13: Floor Plan

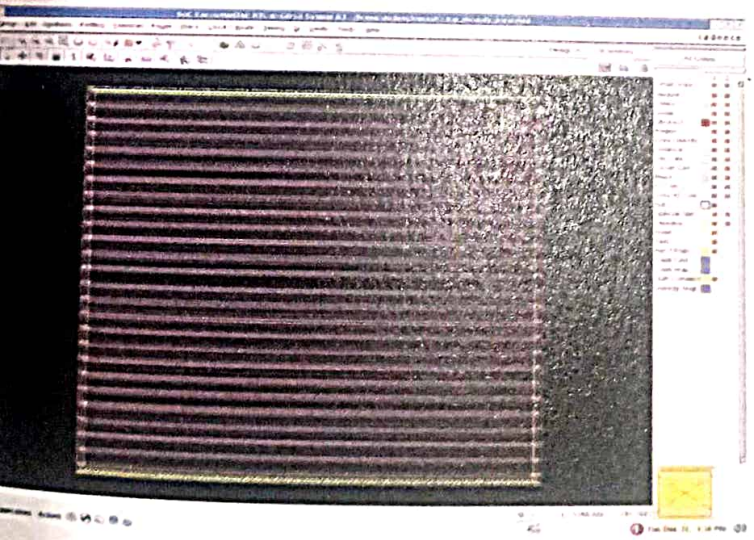


Figure 14: Power Plan

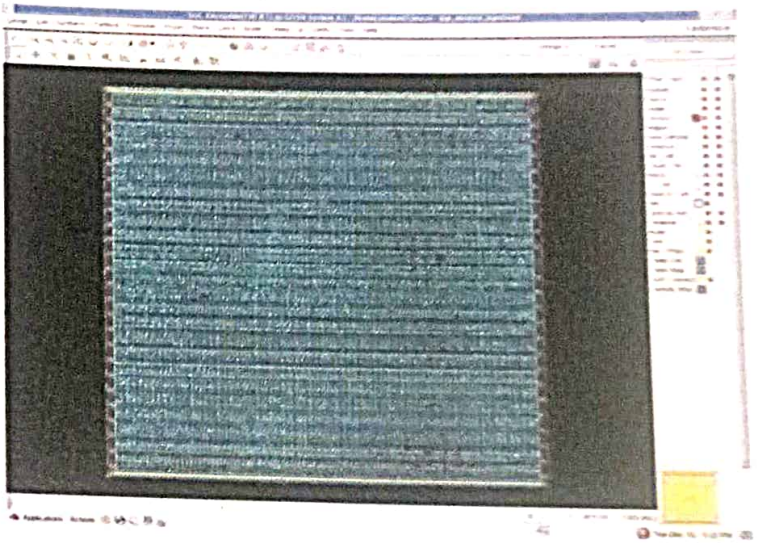


Figure 15: Placement of standard cells

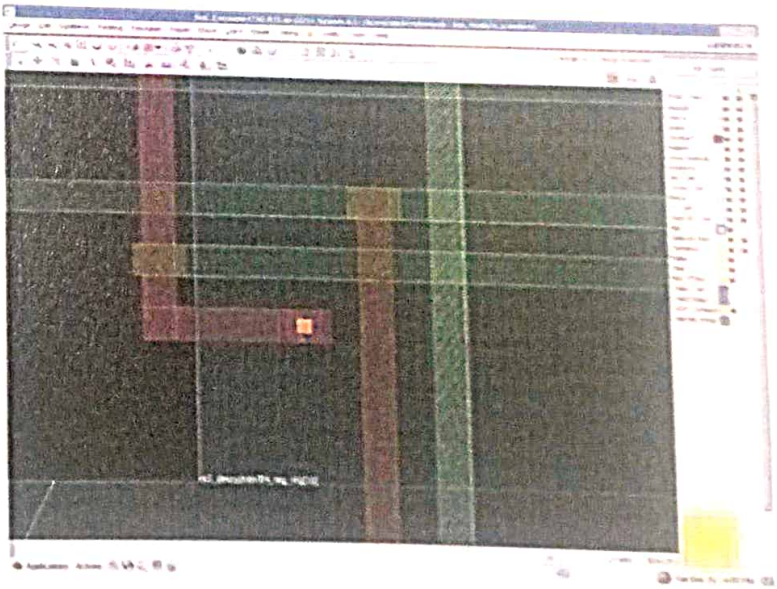


Figure 16: Clock connection to different blocks

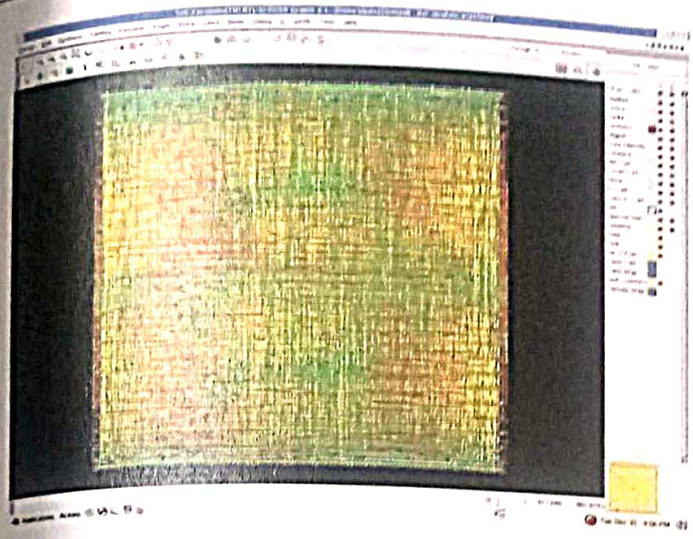


Figure 17: RC5 Routing details

Various reports generated by Cadence SOC Encounter are given below:

Architecture	Gates	Cells	Area
Without pipelining	62116	11996	582300.2 um^2
With pipelining	75502	15360	707785.9 um^2

Table 2: Area Report

Architecture	Internal power(nw)	Switching power(nw)	Leakage power(nw)	Total power(nw)
Without pipelining	36.09	120.8	0.001533	156.9
With Pipelining	43.91	141	0.002109	184.9

Table 3: Power Report

Architecture	Throughput
Without pipelining	5.5 Gbps
With pipelining	10.86 Gbps

Table 4: Timing Report

V CONCLUSION

In this paper, the RC5 block cipher in ASIC Design approach with some optimization techniques to optimized area, power and speed is implemented. The simulated waveforms for the different values of key and inputs are observed so that it provides high security when suitable value of parameter is selected according to requirement of a particular application. With the application of pipelining latency is introduced but throughput is increased by a significant margin. The proposed design is mainly used for transmission security application, by increasing the RC5 encryption algorithm parameter values it is possible to make it suitable for more number of applications such as ATM cards and electronic commerce.

REFERENCES

[1]. B. Schneier, Applied Cryptography, Protocol, Algorithms, and Source Code in C, John Wiley & Sons, 1994.

[2]. H.M. Heys, "Linearly weak keys of RC5", *Electronics Letters*, vol.-33, pp. 836-838, 1997.

[3]. Hu Yupu, Xiao Guozhen. symmetric key cryptography. *[M] China Machine Press*, pp. 144-145, August, 2002.

[4]. R. L. Rivest, "The RC5 encryption algorithm," in Proc. 1994 Leuven Workshop on *Fast Software Encryption*, vol. 1008, pp. 86-96, Springer-Verlag, 1995.

[5]. A. Schubert, W. Anheier, implementation of modern symmetric block ciphers", Electronics, Circuits and Systems, 6th IEEE International Conference61 on Proceedings of Electronics, Circuits and Systems(ICECS), vol. 2, pp.757-760, 1999.

[6]. K.M. Rudrappa, Dr. H.D. Maheshappa, Dr. C. Puttamadappa, K. Somashekar, Venkatesh Prasad K.S., "Implementing RC5 protocol for remote control applications", *International Conference on control Automation, Communication and Energy Conservation (INCACEC)*,pp. 1-6, 2009.

[7]. Chou Fan, Jin Tan, Peng Zheng, "Low-speed wireless networks research and simulation based on RC5", *5th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2009.

[8]. S. Ramachandran, "Digital VLSI system Design" ISBN 978-1-4020-5828-8(HB), 978-1-4020-5828-5(e-book), Springer 2007.

[9]. J. Liang, Q. Wang, Q.Yue, Feng Yu, "An area optimized implementation of cryptographic algorithm RC5",*5th International Conference on Wireless Communications,Networking and Mobile Computing*, pp.1-4,2009.

KIET IJCE KIET International Journal of Communications &Electronics
Volume. No. 2, Issue No. 2, July - Oct 2014, ISSN: 2320 - 8996

Analysis of Microstrip Filters Using Metamaterial Applications

Navita Singh[1], R.N.Baral[2], Arun Kumar[3]

Department of Electronics Engineering, I.F.T.M. University, Moradabad, India[1]
Department of Electronics Engineering, I.M.S. Engineering College, Ghaziabad, India[2]
Department of Electronics Engineering, I.F.T.M. University, Moradabad, India[3]
singh.navita@rediffmail.com[1], r.n.baral@gmail.com[2],
drarunkumarakp@gmail.com[3]

ABSTRACT—**In this paper, a review has been presented on microstrip technology with the using of Metamaterial applications. Metamaterials are special category of artificially engineered structures with sub-wavelength unit cells .In recent years, research on metamateials, especially on left handed materials (LHMs, i.e. Metamaterial with simultaneously negative electrical permittivity and magnetic permeability has aroused much interest due to the many involved physical properties such as refraction.**

Keywords — Metamaterial, Microstrip filters, Resonators, Negative Refractive Index.

I. INTRODUCTION

Metamaterials refer to artificial structures that consist of a periodic array of metal pieces or the like. Technologies called "left-handed Metamaterials" in particular can even produce phenomena that are not available in natural substances and thus it is expected that this will enable the fabrication of electronic devices with functions heretofore unimaginable.

This paper first provides an overview of what left-handed metamaterials are and then introduces technologies that are nearing practical use, focusing on such applications as telecommunication devices, we will also mention the future evolution of such technologies, and the trend of research papers on metamaterials. Metamaterials are usually composed of periodic sub-wavelength units, which can produce electric or magnetic response under the excitation of external incident waves. Since the characteristic dimensions of the composing units are far smaller than the working wavelength, effective medium theory can be utilized to describe the electromagnetic properties of the periodic structures. A number of applications have been verified by experiments like invisible cloaks, microwave lens and tunnelling structures [1-3].

II. BASICS OF METAMATERIALS

The word "meta" derives from the Greek word that means "beyond". While conventional materials provide their intended physics properties in terms of design on the atomic or molecular level, metamaterials realize their specified physical properties through the design of an artificial structure that can be regarded as a quasi-uniform medium in a macroscopic view.

Periodically arranged at intervals shorter than the specified wavelength of an electromagnetic wave, small pieces of metal and the like can constitute an artificial medium that has characteristics not found in nature. Such a medium is called metamaterial. Metamaterials can also be made of dielectrics, magnetic substances, semiconductors, and the like, and even electric circuits instead of metal pieces.

III. LEFT-HANDED METAMATERIALS AND CONVENTIONAL METAMATERIALS

Russian scientist V.G.Veslago published about 40 years ago that examined the effects of a "left-handed" material with the simultaneously negative-permittivity and permeability along with a negative refractive index. Having originated from a purely theoretical interest, the study predicted some new phenomena that had never been conceived of. Left-handed materials were supposed to have a negative refractive index and optical applications of their characteristics attracted interest. Since there was no actual material to validate the theory at that time, no further attention was given to left-handed materials.

In 2000, US physicists D.R.Smith et al. Realized a left-handed material by an artificial structure called Metamaterial. A number of discussions and examples of experiments have been reported ever since. The electromagnetic characteristics of electronic material are primarily determined by the basic parameters, i.e. the permittivity, the permeability and the conductivity.

In contrast to such ordinary electronic materials, ones with this simultaneously negative- permittivity and permeability, if any are referred to as left-handed materials since the vectors correspond in direction to the thumb and two figures of the left hand (the third quadrant in Figure 1). There exist no left-handed materials in nature, however. Left-handed materials produce peculiar phenomena among which "negative refractive index" and the generation of a "backward wave" are the properties of particular significance.

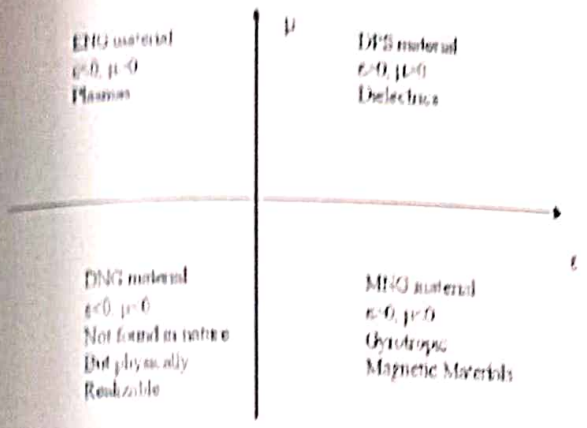


Fig.1. Classification of Materials by Permittivity ε and Permeability μ

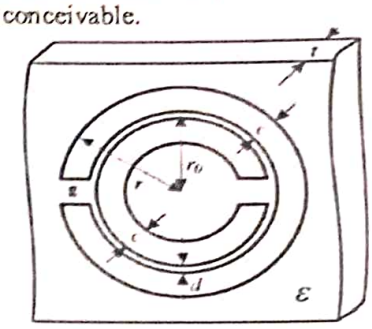
IV. CATEGORIES OF METAMATERIALS

The D. R. Smith's paper of a Metamaterial i.e. a left-handed material consisting of an artificial structure in 200 sparked research into "left-handed metamaterials" for practical use.A left-handed metamaterials is an artificial structure in which small pieces of metal or the like are periodically arranged at an interval shorter than the wavelength of the intended electromagnetic wave. Each individual portion of the periodical structure is called "a unit cell". The left-handed Metamaterial is fabricated by optimizing the shape and arrangement of the unit cells so that the artificial structure has the aimed characteristics.

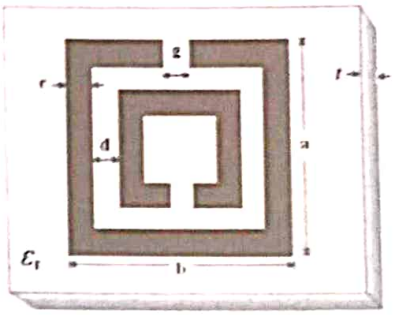
Among the characteristics produced from these artificially-structured metamaterials, left-handed metamaterials are regarded as a technique to make positive use of "dispersion characteristics" that change with frequency. In other words, left-handed metamaterials inevitably have frequency dependencies and show left-handed characteristics in a certain frequency band. It follows that left-handed metamaterials may also show right-handed characteristics or rejection characteristics as well in other frequency bands. In the field of information and communications, many left-handed metamaterials are used in many applications as a combination of left handed and right handed elements, rather than as sole left-handed elements and the former applications are the more dominant in practice. Such metamaterials are some times referred to as CRLH (Composite Right/Left-Handed) metamaterials, where they are categorized as also left handed materials since they include left-handed elements.

V. APPLICATIONS OF METAMATERIALS

A large amount of research works have been done by many research groups around the globe to understand the novel properties of electromagnetic materials and their potential applications in various fields like wireless and mobile communication, medical application, right from the microwave to the optical frequency range especially in designing of filters. Metamaterials are a new class of artificial materials whose microstructure is engineered to exhibit unique electromagnetic properties either rarely, if not, encountered in nature or previously believed to be physically inconceivable.



(a)



(b)

Fig. 2. SRR topology (a) Circle Shape (b) Square Shape.

In 2005, Christophe Caloz and Tatsuo Itoh demonstrate the fundamental aspects of LH/CRLH metamaterials , described some of their applications, discussed potential future devices and structures and has anticipated some of the challenges toward a brilliant future. It is believing that Metamaterial have a huge potential and may represent one of the leading edges of tomorrow technology in high frequency electronics [6].

In 2011,Vipul Sharma et.al, introduce conventional SRR which shows negative permeability at a narrow magnetic frequency resonant band and to obtain LHM, an additional metallic rod is to be incorporated with the SRR for electrical resonance(negative permittivity) while the ESRR structure gives LHM response without using any additional metallic rod. This type of ESRR can be easily incorporate with microstrip antennas to get highly directional beam pattern because of NRIM properties of ESRR. These types of planar microstrip structures are very useful for applications where space of equipment is a constraint. Here structure is inspired by SRR it does not incorporate additional metallic rod for electrical resonance as used with conventional SRR. The rings are elliptical in shape and coaxial dual feeding has been used that are offset in phase.

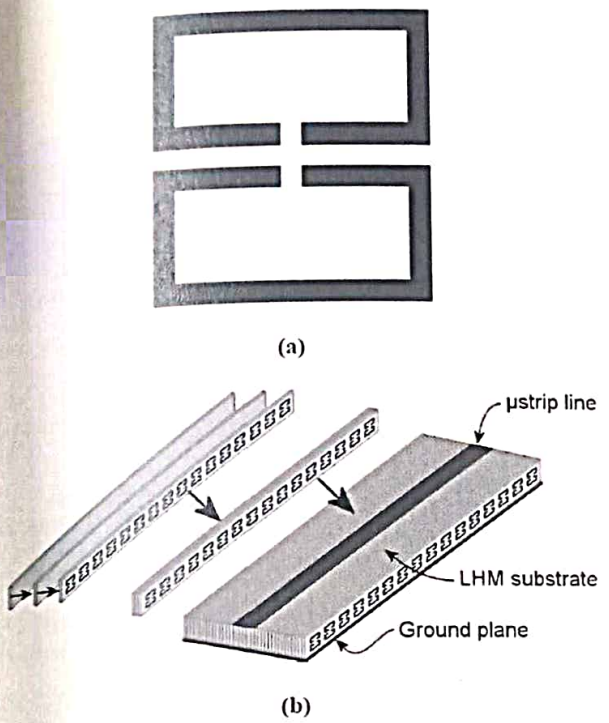


Fig.3 a) Symmetric split ring resonator b) metamaterial substrate constructed by combining dielectric strips with SSRRs.

In 2005, J.D.Baena, et.al. proposed a new approach for the development of planar metamaterial structures. The analyzed structures are based on the coupling of SRRs & CSRRs to conventional planar lines. They are fully planar i.e. they neither incorporate vias, nor other non planar inserts nor can be implemented in both CPW and microstrip technology. By properly coupling SRRs or CSRRs to a host planar transmission line, planar structures with effective negative constituent parameters can be obtained. These structures are fully planar (i.e. without vias or other no-planar objects) and can be easily fabricated by using standard photo-etching technique.The main purpose of this paper is to provide simple and analytical techniques for the design of these structures. These techniques are based on lumped-element circuit models, able to describe the elements and their coupling to the host transmission lines, as well as on analytical formulas to determine the main circuit parameters for these models [7].

In 2006, J. Bonache, I. Gil, J. Garcia-Garcia, and F. Martin proposed a new design approach, based on the use of CSRRs for the synthesis of compact microstrip filters. This was the first time that planar filters with controllable bandwidth based on CSRRs were achieved. Under this design method, the basic filter cell was designed such as to consist of an arrangement of grounded stubs, CSRRs and series capacitive gaps. The introduction of shunt stubs potentially provided capability to synthesize frequency responses with compact dimensions and controllable bandwidth. A equivalent circuit model for the basic filter cell has shunt stubs and series gaps have been represented by inductor (lumped) and capacitors respectively and the CSRRs have been modelled by parallel resonant structure. The structure is composed of periodic structure and behaves as a LH-TL with controllable BW [10].

In 2013, Hichqm Lalj, Hafid Griguer, M'hamed Drissi, proposed a design where two techniques are used for the metamaterial miniaturization, to optimize the physical and electrical size of the CSRR. The band stop filter is produced by an array of miniaturized loaded CSRRs etched on the centre line of a microstrip. The size of the proposed filter is as small as 0.58 cm^2 and its electrical length is very small with only 0.08 λ compared to the conventional band stop filter, a miniaturization of a factor five while the performance is maintained [11].

In 2013, Lakhan Singh and P.K.Singhal, discuss two microstrip band pass filters. One is cascade trisection filter without split ring resonator and other is with split ring resonator and after simulation compared their results. The simulated result shows that by using rectangular split ring resonator inside the split ring resonator the fractional bandwidth is increases and the return loss in the pass band is also increase and the rejection in the lower side of the pass band is also increases. The filter without SRR is resonating at frequency 1.4 GHz with return loss -20dB where as the filter with SRR is resonating at frequency 2.05 GHz with return loss -31 dB in the passs band. The filter with SRR giving fractional band width of 10% as compared to filter without SRR having fractional band width is 8.5% [12].

VI. CONCLUSION

Metamaterials and especially left-handed metamaterials present a new paradigm in modern science, which allows to design novel microwave components with advantageous characteristics and small dimensions.
Due to the small electrical length of the resonators employed, the presented approaches become very attractive for the design of compact planar microstrip filters using metamaterials. If practical applications to exploit the advantageous properties of left-handed metamaterials for the market requirements are proposed by industry without being blinded by the linear model of research and development and if academic societies work cooperatively with the proposals, there will be then technical advances promoting its practical use and even another step forward. With the globalization of research activities and worldwide competition, the speed of development has grown intense.

REFERENCES

[1] Schurig.D., Mock.J. J., Justice J.B., Cummer A.S., Pendry.B.J., Starr. F. A., and Smith. R. D., 2006 "Metamaterial Electromagnetic Cloak at Microwave Frequencies," Science, Vol 314, pp. 977-980.

[2] Liu Ruopeng, Cheng Qiang, Chin. Y.J., Mock.J. Jack, Cui Jun Tie and Smith. R. David, 2009 "Broadband Gradient index microwave quasioptical elements based On non resonant metamaterials," Optics Express, Vol.17, pp. 21030-21041.

[3] Veselago. G.V., 1968 " The electrodynamics of substances with simultaneously negative value of ε and μ,"Sov. Phusics Uspekhi, Vol.10(4), pp. 509-514.

[4] Liu Ruopeng, Cheng Qiang, Hand.T., Mock.J. Jack, Cui Jun Tie, Cummer A.S.,and Smith. R. David, 2008 "Experimental Demonstration of Electromagnetic Tunneling Through Epsilon – Near-Zero Metamaterial at Microwave Frequencies," Phys. Rev. Letter, Vol. 100, pp. 023903.

[5] Caloz Christophe, and Itoh Tatsuo, 2005 " Metamaterials for High Frequency Electronics", Proceeding of the IEEE, Vol.93(10), pp.1744-1752.

[6] Marques Ricardo, and Baena Domingo. J., 2004 "Left-Handed Metamaterial based on Dual Split Ring Resonators in Microstrip Technology", Published in URSI International Symposium on Electromagnetic Theory EMTS, pp.1188-1190.

[7] Pendry, B.J., 2000 "Metamaterials and the Control of Electromagnetic Fields", Physics Review Letters, Vol.85(18), pp.1-11.

[8] Gill. I, Bonache. J,Garcia-Garcia. J., Falcone .F, and Martin. F.,2005 "Metamaterials In Microstrip Technology for Filter Application", IEEE Transactions on Microwave Theory and Techniques, Vol. 1A, pp.668-671.

[9] Baena.D.J., Bonache Jordi , Martin Ferran, Sillero and Ricardo Marques,2005 "Equivalent Circuit Models for SRRs and CSRRs Coupled Planar Transmission Lines", IEEE Transactions on Microwave Theory and Techniques, Vol-53(4), pp.1451-1459.

[10] Bonache. J.,Gil. I.,Garcia-Garcia. J.,and Martin. F., 2006" Novel Microstrip Band PassFilters Based On Complementary Split Ring Resonators", IEEE Trans. Microwave Theory Tech.,Vol.54(1), pp. 265-271.

[11] Lalj Hichqm, Griguer Hafid, and Drissi M'hamed, 2013"Very Compact Band stop filter Based On Miniaturized Complementary Metamaterial Resonators", Wireless Engineering and Technology, Vol.4, pp.101-104.

[12] Singh Lakhan, and Singhal P.K., 2013, "Design of Bandpass Cascade Trisection Microstrip Filter", International Journal of Engineering and Science, Vol.2 (3), pp.104-107.