ULTRASONIC RADAR NAVIGATION USING RC4 ALGORITHM FOR SECURITY

[1]Dhanlakshmi C. Hedgire, [2]S. S. Killarikar

[1]M. E. Student, [2]Professor

[1]Department of Electronics and Communications Engineering,

[1]M. S. Bidve Engineering College, Latur, Maharashtra.

Abstract : Nation's security is an important factor in today's enemy warfare. To improve the war technique and reduce the man power this work is proposed. This paper is based on Ultrasonic radar navigation system. The important and vital role is played by military based surveillance radar which is implemented using ARM7 board. This paper deals with an idea of detecting the incoming object whether it is enemy or friendly using encryption and decryption techniques and if the detected object is enemy then it destroys the object. The ARM7 board is used for the reason of its low cost. The ultrasonic radar system continuously scans and detects object. It also determines the incoming object is friend or enemy using RC4 algorithm which is implemented in ARM7. RC4 is preferred due to its simplicity and speed and it can be efficiently implemented in hardware as well as software. Wireless IR transceiver module is used for security data transfer between transmitter and receiver.

IndexTerms **- ARM 7, RC4 algorithm, Ultrasonic Radar model, IR module, Ultrasonic Sensor, Visual basic (VB) software.**

I. INTRODUCTION

Radio detection and Ranging (RADAR) are remote sensing system used in different applications such as commercial, scientific and military. Radar uses radio waves to determine the range, altitude, direction, or speed of objects in object detection system. Navigation is related to the process of monitoring and controlling the movement of a craft or vehicle from one place to another. Navigation plays very important role in border security system. The field of navigation includes categories like land navigation, marine navigation, aeronautics navigation and space navigation.

It is important to develop a complete independent system that will automatically recognize, track and destroy the incoming object in predefined area under surveillance which can also work in adverse environmental conditions where it is hard for a human soldier to fight with enemy. Entry restricted areas such as Line of Control need to be safe from enemies.

Cryptography is very important in border security system and it keeps every data confidential between sender and receiver so as data is more secured and no one can hack this data easily. In defence system to detect object accurately the combination of navigation technique and cryptography concept is used. For effectiveness of the system target accuracy is a critical factor. Encryption key is used for Encryption and this specifies how message is to be encoded. An authorized party is able to decode this encoded message using decryption algorithm, which can be only decoded with a secret decryption key.

II. BACKGROUND AND RELATED WORK

In paper [1], the objects can be detected, tracked and destroyed by capturing an image with the camera kept in some fixed suitable place, from which complete and clear view of the area under surveillance. It is very difficult to detect an object with the camera in adverse environmental conditions and in night situations. In paper [2], it detects exact kind of obstacles and its count by means of camera and image processing, the fundamental principles of radar and image processing are used in combination to make a system which prevent terrorism.

In paper [3], The RC4 algorithm is better than AES. The RC4 algorithm is well suited for real time processing because it is faster, easier than AES and energy efficient for encryption and decryption.

In paper [4] [5], the position of missile navigates as per the user's requirement by sending the co-ordinates through pc based server on the base station. For security purpose encryption is done with RC4 algorithm and pic microcontroller is used. It uses Human Computer Interaction and Visualization technology. The most important factor is security of data for military applications and it is done by entering the position, an angle of missile and giving directions such as forward/ reverse, left/ right directions of missile onto user interface. For secured data transfer zigbee module is used [6].

In paper [7], the distance is measured between ultrasonic transmitter and receiver units mounted at a small distance by using ultrasonic sensors and microcontroller. Ultrasonic sensor is having low cost hence it is used for measuring the distance. Ultrasonic sensor transforms an electrical signal into ultrasonic waves and vice versa, same sensor can be used for transmitter part as well as receiver part [8]. Ultrasonic sensor is applicable in many areas like in private housing, health care, defence system. RADAR are remote sensing system with military, scientific and commercial applications, EM waves are sends by the Radio detection and ranging. Some developments of radar are Radar networks, Security and privacy, Navigation and positioning (localization), In-network information processing, Target detection and tracking and other various applications [9].

III. PROPOSED SYSTEM

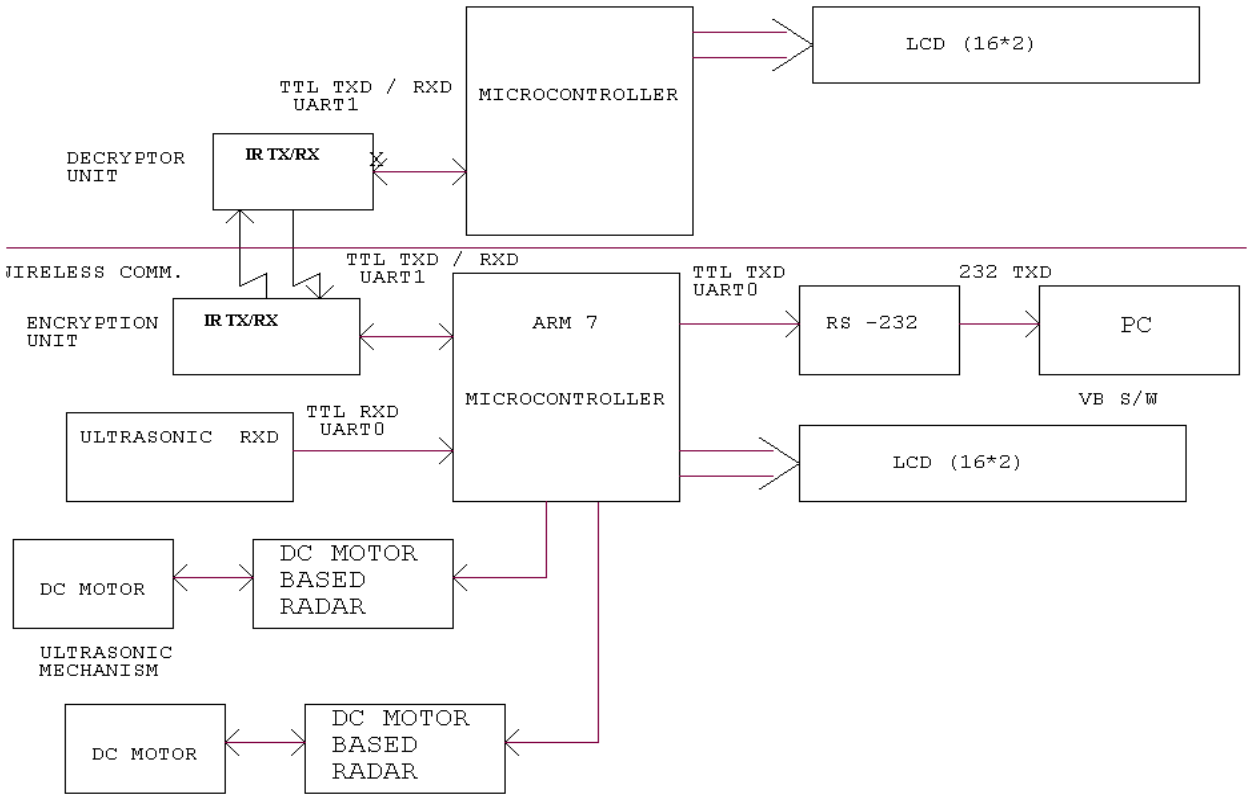

Fig. 1 Block Diagram of the system

The above Fig. 1 shows the block diagram of proposed system in which lower part of the diagram is transmitter side which consist of ultrasonic radar model for detecting obstacles, ARM for encryption, LCD to display distance of the obstacle from the radar tank and IR module for transmitting the encrypted frame. The upper part of diagram is receiver side and it consist of ARM for decryption, LCD for displaying output and IR module for sending decrypted frame to the transmitter.

IV. HARDWARE DESCRIPTION

The hardware can be described in 3 units.

Tank unit:

Here we are making a robotic tank unit which is having 2 DC motor based tires and which helps to move the radar in forward, reverse, left and right direction.

Ultrasonic based Unit:

Here we are developing a radar unit which will have a DC motor and which will rotate in 360 degrees in clockwise as well as anticlockwise direction. The DC motor continuously rotate the whole mechanism containing the ultrasonic radar model and ultrasonic sensor will continuously send and receive the ultrasonic waves (of 40 KHz). The Doppler effect is used to calculate the distance and measured distance is directly given to the ARM µC. The ARM µC receives the distance from ultrasonic sensor serially and transmits it to on board PC. The PC is having VB software used to show the position of the incoming object graphically and it will continuously monitor the obstacles distance, distance and angle reading can be viewed on it send by the µC. The µC will then calculate the distance and display the object distance on LCD. If the measured object distance is less than the threshold, then the radar stops and the ARM7 will send an encrypted frame wirelessly towards the approaching tank unit through IR transceiver. The IR module will transmit the encrypted frame wirelessly.

Approaching Tank Unit:

Here the ARM7 µC is interfaced to the IR transceiver unit and when the encrypted frame is received by the ARM7 µC via IR module, the received encrypted frame is decrypted by on board µC and then sent back to the tank using the same IR module.

V. RC4 ALGORITHM

The RC4 Encryption Algorithm, developed by Ronald Rivest of RSA, is a shared key stream cipher algorithm which requires a secure exchange of a shared key. The key algorithm is used for encryption and decryption as the data stream is simply XORed with the generated key sequence. This algorithm is serial as it requires successive exchanges of state entries based on the key sequence. This encryption and decryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol). The RC4 algorithm works in three parts as follows.

1. *The key scheduling algorithm*

Initialization:
For i=0 to 255 do
$S[i] = i$;
$T[i] = K[i \bmod keylen]$;

end

Initial Permutation of S:
j=0;
for i = 0 to 255 do
j=(*j* + *S*[*i*] + *T*[i]) mod 256;
Swap (*S*[*i*], *S*[*j*]);
end

2. *The pseudo-random generation algorithm*

Generation loop:
i, j = 0;
while (Generating Output)
i = (*i*+1) mod 256;
j = (*j*+*S*[*i*]) mod 256;
Swap (*S*[*i*], *S*[*j*]);
t = (*S*[*i*] + *S*[*j*]) mod 256;
k = *S*[*t*];
output k
end

3. *Encrypt using XOR operation*

The generated key sequence by using KSA and PRGA algorithms is simply XORed with the plain text to get the encrypted message or unreadable cipher text.

Flowchart of RC4 algorithm:

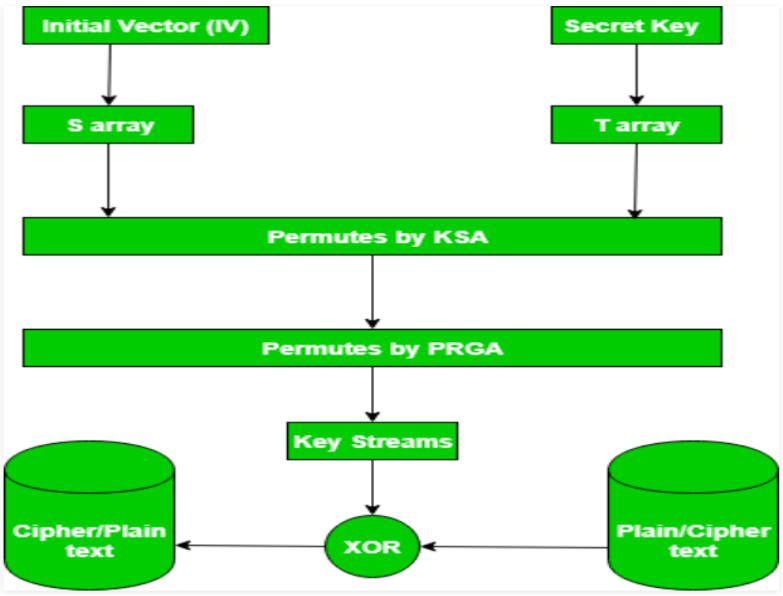

Fig. 2 Flowchart of RC4 Algorithm

Algorithm features:

It uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. This state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Here each element in the state table is swapped at least once.

This key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128-bit key. It has the capability of using keys between 1 and 2048 bits. RC4 algorithm is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.

This algorithm works in two phases that is key setup and ciphering. Key setup is the first phase of this encryption algorithm. During a N-bit key setup (N being key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of operations like swapping bytes, modulo operations, and other formulas. A modulo operation is the process of taking a remainder from division. For example, 11/4 is 2 and remainder is 3; therefore, it would be equal to three.

VI. SOFTWARE DESCRIPTION

The ultrasonic radar model continuously captures the signal using ultrasonic sensor and measures distance from incoming object is to be transmitted to transmitter. Once the signal is captured ARM µC is initialized. Also the distance is displayed on LCD. If measured distance is less than set point, then ARM µC sends encrypted frame to the IR transceiver through UART. The detected objects are also displayed on PC having VB software. All the initialization of UART, Timer and LCD is done in Embedded C using Keil µvision3. RC4 algorithm is also done in Embedded C using Keil in which 256 state and 4-bit key is used for encryption and decryption. VB software is used to plot the obstacles graphically on PC.

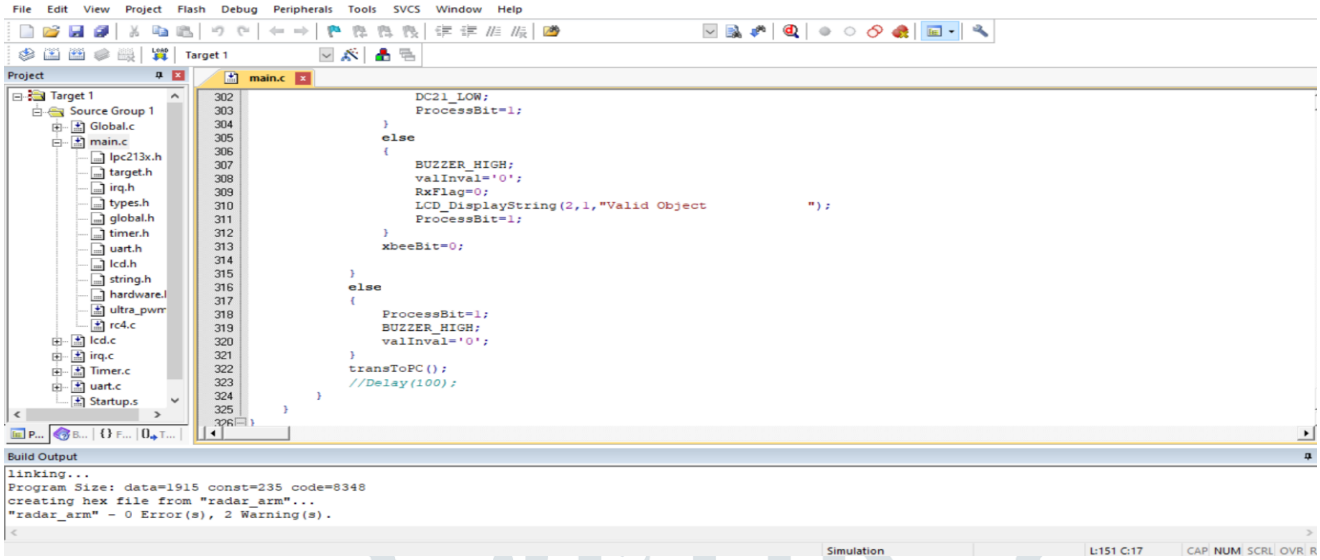

Fig. 3 Screenshot of the code after debugging (transmitter)

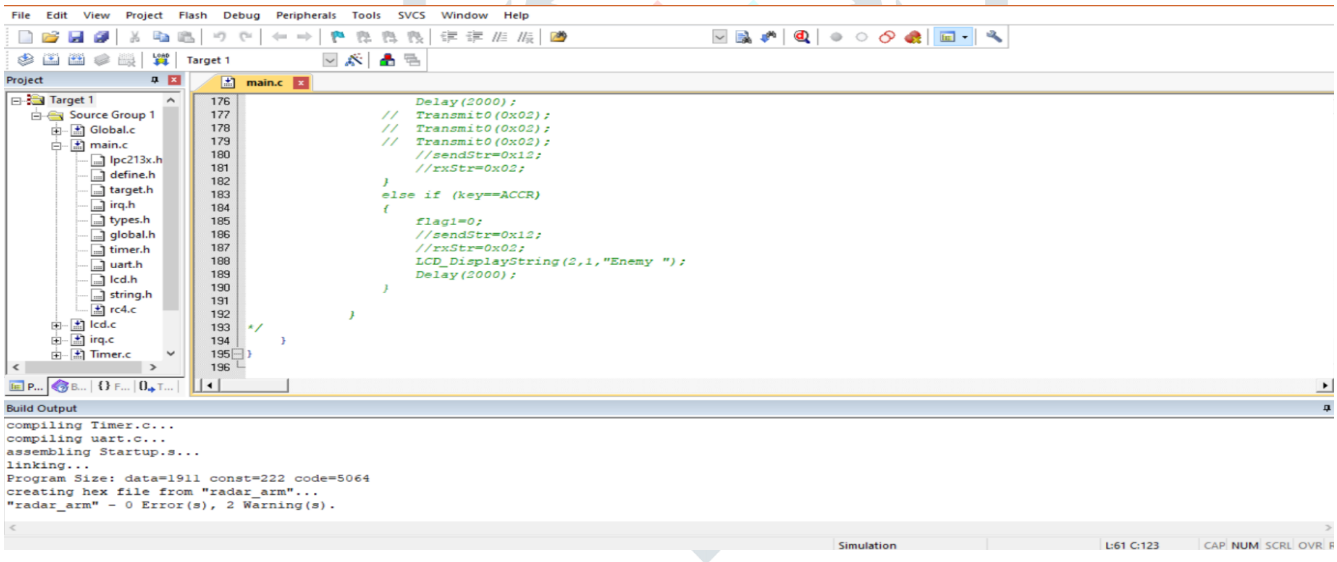

Fig. 4 Screenshot of the code after debugging (receiver)

VII. RESULTS

1. Ultrasonic radar model that is transmitter side which rotates 360 degrees with the help of dc motor, tracks the obstacles in all direction as shown in Fig. 5. The receiver side is as shown in Fig. 6.

Fig. 5 Transmitter side model of the radar system

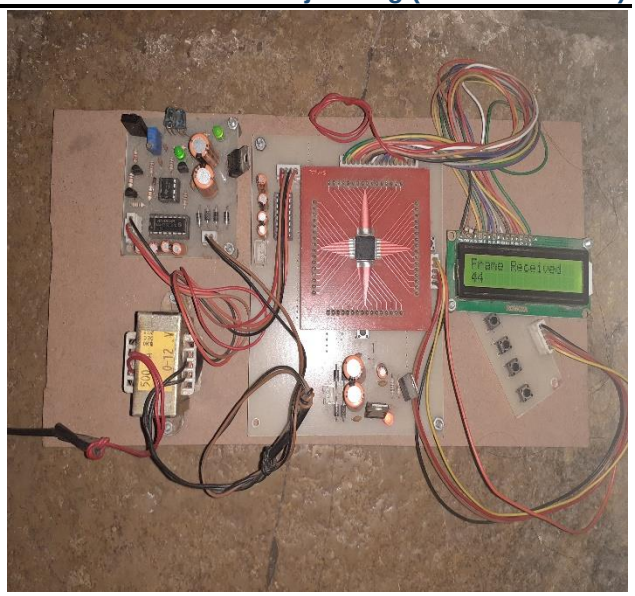

Fig. 6 Receiver side of the radar system

2. When object crosses the set range and detects the obstacle, it displays the message on LCD screen as shown in Fig. 7 and also transmitter sends the encrypted frame to the receiver as shown in Fig. 8.

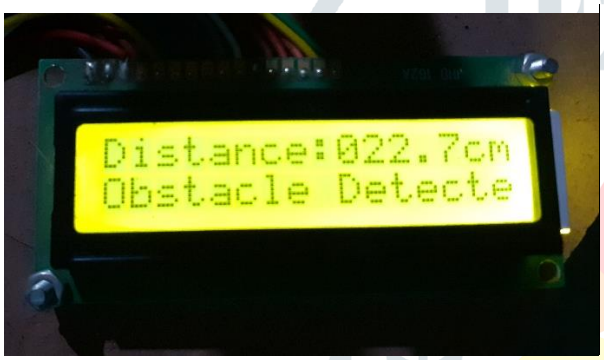

Fig. 7 LCD displays detected object distance

Fig. 8 LCD displays encrypted data from transmitter side

3. When receiver receives the encrypted frame it displays on LCD as shown in Fig. 9 and also displays the response sent to the transmitter as shown in Fig. 10.

Fig. 9 LCD displays frame received

Fig. 10 LCD displays response send to transmitter side

4. If receiver does not send any response to the transmitter, then transmitter displays obstacle invalid as shown in Fig. 11. When transmitter gets response from receiver side then it displays obstacle valid on LCD as shown in Fig. 12.

Fig. 11 LCD displays Invalid object

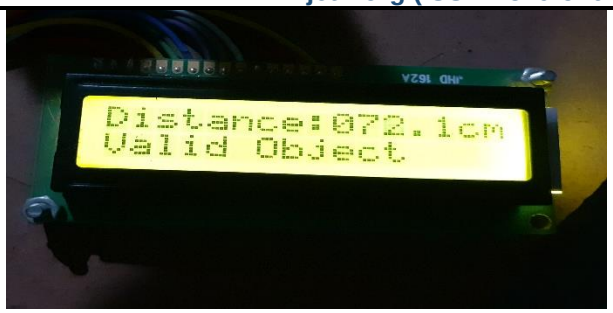

Fig. 12 LCD displays Valid object

5. we have to select proper port to display the distance and angle of the obstacle from radar on PC as shown in Fig. 13 and Here tracking and monitoring of obstacle is displayed on PC having visual basic software as shown in fig. 14.

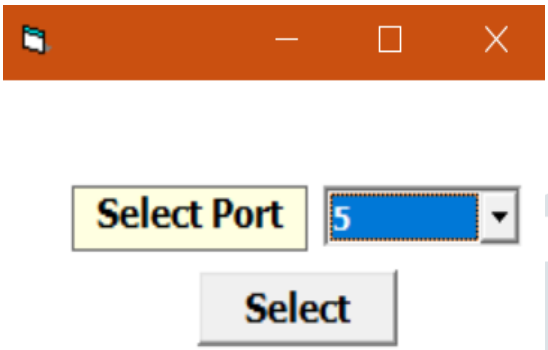

Fig. 13 Selection of Proper Port

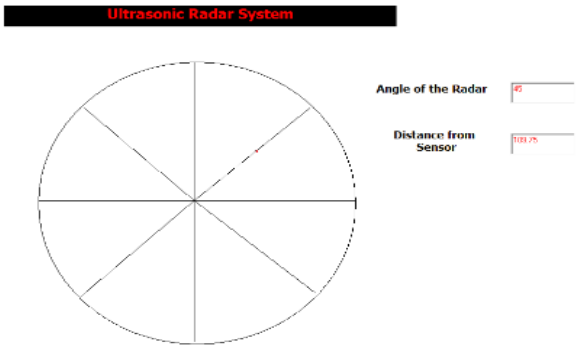

Fig. 14 PC shows position of obstacle

VIII. Conclusion

This paper gives accurate detection and authentication of target object. The accurate target object is detected by the ultrasonic radar model and RC4 algorithm is used to determine the detected object is friend or enemy. RC4 algorithm is easier, fast and also provides more security. In this paper, the radar having two main parts that is transmitter and receiver. IR transceiver is used for wireless communication between transmitter and receiver. PC is having VB software which continuously scans and monitors the position of obstacle. It gives the visual description of incoming object. However, image processing proves to be time consuming for fast detection of objects as well as become difficult in adverse weather condition, hence this system becomes very useful in night situations, adverse weather condition or smoky battlefield environment where human eye is unable to identify the incoming object.

IX. Future Scope

The visual representation of objects which is observed in visual basic software on PC, with some modifications that may observed on tablet by making application in future. The future modifications may also include addition of specialized cameras, smart phones, voice recognition systems.

X. Acknowledgment

I would like to thank to the HOD and all the staff members of Department of Electronics and Communication Engineering for their valuable support. I also express my sincere gratitude to my guide Prof. Mrs. S. S. Killarikar, Department of Electronics and Communication Engineering for her valuable guidance and support.

XI. References

[1] Amit Kenjale. 2013. Automatic Object Recognition, Tracking and Destruction for military application from World Congress on Information and Communication Technologies.

[2] Supriya Kunjir and Rajesh Autee. 2015. Terrorist Scanner Radar Along with Camera using Ultrasonic Frequency and Multiple Object Detection. International Journal of Advanced Research in Computer Science and Software Engineering, 5(9).

[3] Nidhi Singhal and J.P.S.Raina. 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization from International Journal of Computer Trends and Technology.

[4] Kulkarni Laxmi G. and Dawande Nitin A. 2014. Secured communication for missile navigation from International Journal of Engineering research and General Science, 2(4).

[5] Khole S. W., Chincholkar S. P. and Chaudhri E. M. 2015. Secured Missile Navigation from International Journal of Pure and Applied Research in Engineering and Technology, 3(9).

[6] Murumkar Govind and Nikumbh D. M. 2015. Smart Secured Wireless Communication for Missile Navigation Using RC4 Algorithm from International Journal of Scientific Research and Engineering Studies (IJSRES), 2(2).

[7] Shrivastava A. K., Verma A. and Singh S. P. 2015. Distance Measurement of an Object or Obstacle by Ultrasound Sensors using P89C51RD2 from International Journal of Computer Theory and Engineering, 2(1).

[8] Mansoor-Ul-Hassan Siddique. Ultrasonic Radar and Its Applications from Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications (AIC '09).

[9] Chetana Singh, Abha Agnihotri and Pallavi Patel. 2013. Development of Radar Using Ultrasonic Sensor from International Journal of Advance Research in Science and Engineering Ijarse, 2(10).

[10] Qian Yu and Chang N. Zhang. 2011. RC4 State and Its Applications from ninth Annual International Conference on Privacy, Security and Trust.