International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

Crypto Vision Bot Using RSA Algorithm

Sangmesh Melinmani
Assistant Professor ,
Depatrment of Electronics and Communication Engineering
Dayananda Sagar College Of Engineering
Bangalore,INDIA

Venkatesh.K
Department of Electronics and Communication Engineering
Dayananda Sagar College Of Engineering
Bangalore,INDIA

Yogesh C.R
Department of Electronics and Communication Engineering
Dayananda Sagar College Of Engineering
Bangalore,INDIA

Yogeshwar B.R
Department of Electronics and Communication Engineering
Dayananda Sagar College Of Engineering
Bangalore,INDIA

Prakash V
Department of Electronics and Communication Engineering
Dayananda Sagar College Of Engineering
Bangalore,INDIA

Abstract — *In this world of universal electronics, transmitting private data via a computer network necessitates a high level of security. For clouds, networks, and individuals, researchers are also looking for the most secure and complicated cryptographic methods. Cryptography is the process of converting data or information from one form to another in cryptography, and it is a very efficient and effective technique of securing data. RSA Algorithm will allow for securing the communication when third parties are present. As there is an increased public security awareness a huge demand is essential for any effective surveillance system, it has grown significantly, with the goal of lowering crime rates and serving numerous objectives. However, several developed monitoring systems contain flaws that limit their uses. This project mostly consists of a design and a robot powered by a Raspberry Pi 3B+ with a DC motor, AVR board, Bluetooth, and a Raspberry Pi camera are all used to send live data over a virtual network and update collected photos for encryption and decryption. With the help of communication there is huge advantage for any multimedia systems, medical purposes as well as in military-based imaging systems all use image encryption. This project covers a wide range of electronic and computer science topics, including cryptography and network security, Python programming, wireless sensors, and the Internet of Things.*

Keywords — Cryptography, RSA Algorithm, Encryption, Decryption, AVR board, IOT

I. INTRODUCTION

Information has been one of our most valuable possessions since the birth of civilisation. The ability (or inability) of our species to maintain secrets and hide information has wiped out political parties, turned the tide of wars and toppled entire regimes. Every day banks, payment processors and their clients exchange sensitive financial information. Whether you realise it or not, all of these records must be saved in a huge database at some time. Cryptography, or the art and science of encrypting sensitive data, was traditionally exclusive to government, academics, and the military. These are more important in our daily lives. Digital signatures and authentication are critical applications. This would be a major issue without cryptography a significant issue If any of these documents were stored or communicated without encryption, hackers would have free reign, and your bank account would swiftly deplete. Banks, on the other hand, are aware of this and have gone through a lengthy procedure to implement advanced encryption technologies to keep your information safe from hackers and food on your table. Visual cryptography is a kind of cryptographic technique which is mainly applicable for encrypting visual information like images as well as used in text etc by which the decrypted information appears in the form of an visual image. Visual cryptography is employed in the real of data concealment and authentication in cybercrime. At its most basic level, cryptography consists of two steps: encryption and decryption. A cypher is used in the encryption process. Turn plaintext into ciphertext to encrypt it. On the other side, decryption uses the same cypher to convert ciphertext to plaintext. Cryptography has come to pervade all aspects of ordinary life as a result of recent technical developments. Everything from your smartphone to your banking relies largely on cryptography to keep your information safe and your livelihood secure, and we employ the Mutual Authentication procedure to satisfy all Cryptography

services, such as Access Control, Confidentiality, Integrity, and Authentication. We can keep the data more securely this way. Because we utilise the RSA algorithm to secure the data (pictures), any other individual on the network will be unable to access the data. The goal of this project is to imply a new method of disguising an image by utilising the capabilities of the RSA algorithm in cryptography. RSA(Rivest-Shamir-Adleman) is asymmetric cryptography algorithm which focus to work on the basis of two different keys one is called as Public Key and other is called as Private Key. Here the Public Key is known to all the uses who wants to use the encryption and Private key is the key which is kept private so that presence of private and public key enables a successful encryption and decryption. Nowadays RSA has been still used in a range of many web browsers for secure information purpose ,email for secure mail transfer, VPNs, chat and other communication sources. RSA has been used often to make a strong and secure connections in between VPN clients as well as VPN servers.

We will utilise the Raspberry Pi 3B+ as the main hardware in this project and the model will be equipped with an Pi camera sensor for monitoring purposes. DC motors have been employed for movement, which are embedded with the AVR board and relays. Relay are used for smooth robot movement. To prevent damage to the power source for the dc motor, an AVR is employed. This movement is controlled by a free app called "*Serial Bluetooth Terminal*"that can be downloaded from the Google Play Store. The AVR is connected to the HC-05 so that the android phone and the robot may communicate.. It is one of the strategies for motivating workers to complete tasks efficiently and effectively in order to achieve common goals. It is required for improved performance. The key reason for choosing this project is because Providing protection to personal materials, messages, or digital photos has grown difficult due to recent improvements in crypto analysis. Crypto analysis can quickly expose the existence of data, information, or any other medium. As a result of being exposed to such issues, we decided to work on this project, which involves the entire process of transferring an image from one location to another. where the user can access the info anytime they need it without fear of being hacked.

II. LITERATURE SURVEY

It is a project whose main focus was on building a kind of spying robot which can be utilized for manoeuvring and monitoring in treacherous environment. This robotic system includes a Raspberry Pi which has been interfaced with a DC motors for locomotion purpose, GPS module for tracking the location of the robot, Pi camera for image capturing in dark nights, and IR Thermal camera sensor for monitoring heat objects.To control the motion of the robotic system it can be done with the help of a web application through by utilizing a Wi-fi connectivity. This robotic system is programmed in order to stream all the important live data through a virtual network and keep on updating all the captured images and additionally adding up with the time stamp and the location at certain instances to the cloud. It can successfully transmit all the captured real-time videos and pictures through the thermal vision .It can also be utilized in war zones and extremely dangerous places, this also can be used in observing all the targeted disaster-affected regions which are not adequate over beyond human reach [1]

This project mainly focused on the successful transmission of all the private statistics over the computer network . But it needs a huge protection and providing data protection against all the mischievous third party attacks .To tackle these problem cryptographic algorithms are a boon .There are many algorithms but specially RSA has a set of rules based algorithms which can widely been used in Public Key infrastructure implementations. A several prosecutions have been made to make the use of all the needed four keys for more quicker and more efficient than the real encryption and decryption techniques .It enables the implementation of the necessary operation with the continuous subtraction operation instead of division operation.[2]

The main target for a successful communication is secure and reliable exchange of data that occurs in between the devices is crucial and the information should be maintained over the storage devices ,routing devices as well as the communication which occurs over the cloud. Cryptographic techniques are mainly used to give the security for the transmission of all the crucial data and make sure that the user's privacy is given by storing and transmitting all the private data in a particular format. Using encryption we can only intend user possessing the key can access the information. Homomorphic Encryption (HE) is a advantageous techniques which has been utilized in the past years .HE is either seen in its slow transmission ability or fast key capacity of the decryption .The HE-CRT-RSA, utilizes many multiple keys for efficient communication along with the high security HE-CRT-RSA is observed to be 3–4% faster than the classical Rivest-Shamir-Adleman (RSA). [3]

III RSA ALGORITHM

RSA (Revist,Shamir,Adleman) algorithm is an asymmertic key cryptosystem, which can be found mostly used in the confirming all the fragile data, particularly when a person has sent some data over a highly problematic framework, such as the Internet. RSA was basically origanted by thse scientists R.Rivest, Adi Shamir, and Leonard Adleman of the Technology Institute of Massachusetts in 1977. Since it consist of two keys the public and private key the public key can be issued to anyone ,but since privacy of the sent data is essentail and to protect the private key it is not

shared. The two individuals users and the private keys will encrypt the message based on set rule of rule based algorihms encryption happens where as the opposite key from the other end of user is used to decrypt message is used to unscramble it. This attribute is one of the reasons why RSA has become the most frequently used upside-down estimate: it offers a technique to ensure the protection, decency, validity and non-reputability of products such as electronic trades and data collection. Various protocols like SSH, Open PGP, S/MIME, and SSL/TLS rely upon RSA for encryption and progressed mark limits. Programs are an obvious model that needs to establish a guaranteed relationship over an insecure environment such as the Internet or confirm a mechanized imprint, similarly used to programming rationales. RSA signature checks quite possibly the most consistently achieved activities in information

A. RSA ALGORITHM STEPS

1) We select any two prime numbers (basically large prime numbers) so that it can provide more security.

2) Obtain the value of n using (n = pq).

3) Find out Euler's totient function [φ(n) =(p−1)(q−1)].

4)Choose any random integer for 'e' in the range 1 < e < φ(n) such that gcd (φ(n),e) =1.

5) Calculate 'd' using [d=1 mod(φ(n)]

5) The public key is {e, n} and the private key {d, n} are successfully obtained .

6) Encryption

- Substitute all the needed values in the formula.
- Computes the cipher: C = M^e mod (n).
- The ciphertext is obtained and can be given to the recipient.

7) Decryption

- To compute back the plaintext, use the formula M = C^d mod (n)
- If both public and private keys are correct the encrypted and decrypted information will be same

IV .Block Diagram

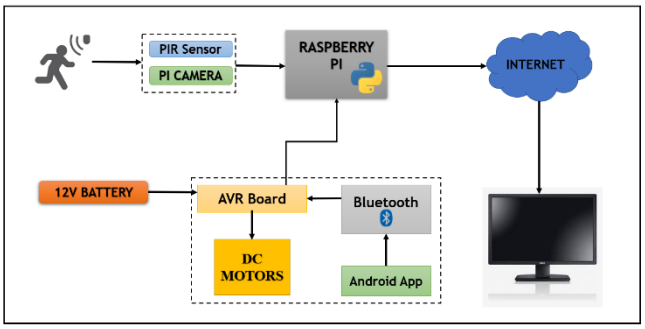

Fig 1: Block Diagram of Robot

All the principal and useful parts of Crypto Bot are referenced in the block graph above. It tends to be extensively isolated into 2 principal parts, the locomotion part and Image Capturing part. For the movement of robot, the modified AVR Board is utilized. This AVR Board comprises of Atmega-48, Relays and Voltage Regulator. The 12V Battery is associated with AVR board. The DC Motors are associated with same source by means of Relay, while Raspberry Pi and Atmega-48 requires 5V Power Supply. This is given with the assistance of Voltage Regulator. The Bluetooth Chip (HC-05) is additionally associated with Atmega-48. The programming of Atmega-48 is done in Embedded C to such an extent that, the total movement of robot can be controlled from an Android App through Bluetooth. This program is dumped into Atmega-48 and the robot is prepared to move.

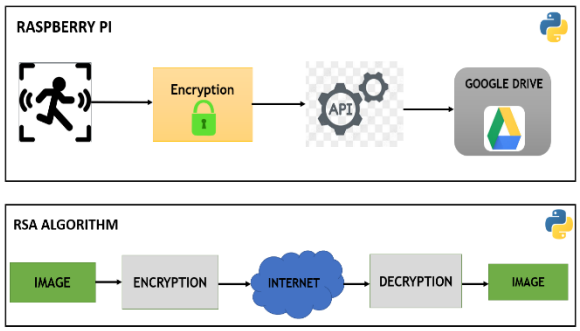

Fig 2: Block Diagram of RSA Algorithm

The Second part is Image Capturing. Here Raspberry PI assumes a significant part. The PIR Sensor is utilized for Motion Detection. When it identifies the movement of any living objects (like Human Beings), it sets off the PI Camera to catch pictures. The caught pictures are examined, encoded and transferred into Google Drive through an API. The encoded picture is put away in the web and just approved client can see this picture. The approved User can utilize Decrypt or program to download and decode the pictures. The program utilizes Google Drive API to lay out Connection and download pictures from

server. The downloaded pictures are then decoded and displayed to User.

At the point when PIR Sensor recognizes the movement, the PI Camera is catches the picture and stores it in SD Card. The picture is presently taken and encrypted utilizing RSA Algorithm. At first the picture caught is gone through an encrypter. The Encryption Algorithm utilizes 4096 bits Public Key to encode the picture. alongside OAEP (Optimal Asymmetric Encryption Padding). The encrypted picture is then transferred to Google drive. We use Google Drive API to lay out secure association with Google Drive and transfer every one of the encrypted pictures. The encrypted pictures can be downloaded on the approved client's machine and decrypted in like manner utilizing Decrypt or Program.

V HARDWARE USED

A. Raspberry Pi 3B+

The Raspberry Pi 3 Model B+ is the important part of the project as it is used to connect Pi camera and PIR sensor to control the image capture and to run the encryption script.

B. Relay

It is a general-purpose switch with a high-current which can be used as a switch to control the dc motors for locomotion purpose.

C. DC motor

Mainly used in a wide range of applications, such as toys and vehicles etc cars which has a 30 rpm which is embedded with the relay.

D. 12V Battery

The battery used is Lead Acid Battery and supplies 12 volts which is mainly used by the DC motor as it required a high voltage used to movement of the robot. And are rechargeable in nature.

E. Jumper Wires

It is enabling a smooth connectivity between each and every component.

F. Pi Camera

Pi Camera module of 5MP is used to take pictures as well as a high definition video and has been connected with the Raspberry Pi Board.

G. PIR sensor

Passive infrared (PIR) sensor are most often used in motion detection purpose with a range of 10 meters and operated at 5V.

H. HC-05

It is used to manually control the locomotion of robot with a frequency of 2.45GHz and range is up to 10 meters.

I. AVR board

AVR is a microcontroller of the ATMEL family, uses at mega 48 microcontroller for controlling the locomotion and Bluetooth

VI SOFTWARE USED

A. Python

The encryption and decryption script is written in python and loaded in raspberry pi and also to control the Pi camera with PIR sensor

B. Embedded C

The AT mega 48 chip is programmed with embedded C to control the robot.

C. Code Vision AVR

It is a cross compiler used to code embedded C to ATmega 48.

D. Raspberry pi OS

Raspbian OS is an open-source computer operating system which is loaded to raspberry pi board.

E. Google Drive API

It is mainly used as a stage by the user to view the decrypted original image.

VII IMPLEMENTATION

It has mainly the two Hardware system :-

i)AVR Board

ii)Raspberry pi

The AVR board is mounted with ATmega 48 IC chip , which has a voltage regulator which helps to regulate the voltage to 5V .Since we are using 12V battery mainly for the movement of the robot we require 12V hence to regulate it for 5V the voltage regulator helps to provide 5V to AVR board which is connected to Bluetooth HC-05.

There are four DC motors where the each side of 2 parallel motors are shorted together and given to relay output pin and VCC to no pin and GND to µc pin within the relay .the ports are declared and given to k1 to k4 as i1 to i4 in the relay from AVR board. The HC-05 module is used

for communicating with the bot using android application called as " Serial Bluetooth Terminal " which is freely available in the Playstore. These components are connected by wires and are placed upon a metallic insulated chassis frame and the chassis is connected with L clamp on all the sides to connect dc motor with movable wheels.

The Raspberry Pi is embedded with the sensors like PIR sensor as motion detector and Pi camera to capture the image. We can observe that whenever any person is standing in front of the robot , it can easily detect the person with the help of PIR sensor ,as a result it triggers the Pi camera to capture the image .Once the image is captured it starts to encrypt using public key and if the private key is utilized by authorized person then he can use that to decrypt the image and can view it in the laptop

In the software implantation , the AVR is programmed with Embedded C programming using code vision .The project file is created by selecting ATmega 48 and set clock to 4 MG Hz in the configure project and by importing the USART protocol, port pins for necessary components and ADC pins selection and the program is written for the locomotion by assigning condition to the port pins and creating necessary function to the direction. After the program is saved as a hex file and dumped to the AVR board using AVR studio application.

For the Raspberry Pi 3B+, the Raspberry Pi OS is loaded in to it .The necessary condition for image capturing from Pi camera and motion detection using PIR sensor is written along with the code for encryption and decryption using RSA algorithm is written and later it is loaded to the raspberry pi board. Once when an motion is detected and image is captured the image gets encrypted using public key which is available to all .If any person without private key tries to decrypt the image he cannot view the it .The image can be viewed by the user using google drive API where he should use the private key. Since the private key is available only with authorized person, he can view it in Google API by which any tampering can be prevented.

VIII RESULTS

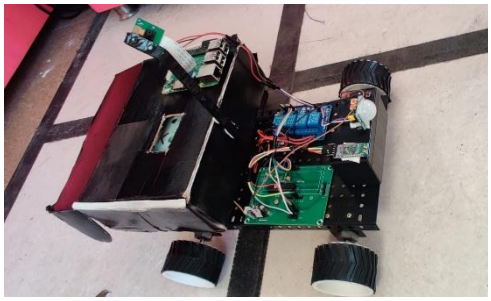

Fig 3: Crypto Vision Bot

Indicates the entire crypto vison bot where the robot is been embedded with all the hardware as well as software connections as mentioned above.

Fig 4: Serial Bluetooth Terminal

It shows the connectivity as well as the movement of the robot in the specified directions using the HC-05 bluetooth in connection with the Serial Bluetooth Terminal App downloaded from Playstore

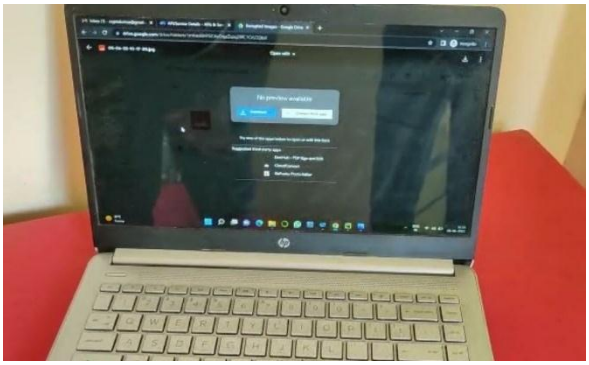

Fig 5 : Encrypted image

The image captured by the Pi camera is been encrypted using RSA encryption algorithm such that encrypted image is not in the format to be viewed

Fig 6: Decrypted image

The authorized person who has the private key can decrypt the image and can view the image captured by the Pi camera

IX ADVANTAGES

- Cost Efficient - Connecting these elements to form a triangle clearly defines costs-benefits, resources-benefits, and costs-resources
- No Data Infiltration - By the help of strong encryption technique ,no one can modify the original information
- More Secure - We are using RSA secure algorithm for information safety
- Authentication - Sensitive information can be accessed only by the authorised person

X APPLICATIONS

- Military Purpose - Our robot is highly recommended for Military security for the Border surveillance, Spying, patrolling this single robot avoids the risk of soldiers
- Cyber Safety and security - due to the excessive leakage of the crucial and sensitive information form in the security area our bots provides better authenticity
- Private investigation - This bots can be used for any kind of investigations in the areas like where human can't visit and collect clues
- Image based automatic inspection and analysis - In our Robot we are using Pi camera to capture image so by using this technique we can inspect and analyses present conditions of the area
- Government department - for enhancing security and safety in government or any civic spots

XI CONCULSION

The proposed framework is endeavouring a cost-effective and feasible project in which the speed of the on RSA algorithm by providing the security for the data by using the two keys those are Public key and the Private key. which is fast efficient and secure wireless communication system. By the use of Pi camera it has ability to capture the image and encrypt using RSA algorithm. This will definitely enable the robot Wireless manual control via web app, live streaming of images Used manually for civilian and military applications through the Firebase platform.

This kind of robots are more effective where human surveillance is hazardous. Mainly our Crypto bot can be easily control by the Android application from the Operator so, the movement of the robot is traceable . Our Robot provide integrity, confidentiality and authenticity from the unauthorised use

XII REFERENCES

[1] Aarthi V, Vishal R, Nagarajan K.K "Smart Spying robot with IR Thermal Vision ," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)

[2] K Pavani, P. Sri Ramya " Enhancing Public Key Cryptography using RSA ,RSA-CRT and N-Prime RSA with Multiple Keys ", 2021 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)

[3] Rabia Abid, Celestine Iwendi, Abdul Rehman Javed, Muhammed Rizwan , Zunera Jalil, Joseph Henry Anajwmba , Cresantus Biamba "An Optimised homomorphic CRT-RSA algorithm for secure and effective communication ", Springer , 2021