



**L** OVELY  
**P** ROFESSIONAL  
**U** NIVERSITY

---

# **B-E&D and E-O Toggle Approach for Image and Text Embedding with ECC**

A Dissertation Report  
Submitted

By

**ABHISHEK KUMAR (11104802)**

To

**Department of Computer Science & Engineering**

In partial fulfillment of the Requirement for the Award of Degree of  
**Master of Technology in Computer Science**

**Under the guidance of**

**Ms. Shabnam Sharma**

(Asst. Professor, Department of Computer Science)

**(May 2015)**

School of: Computer Science & Technology Engineering

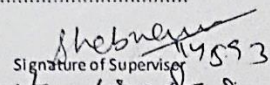
DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Abhishek Kumar Registration No.: 11104802  
 Batch: 2011 Roll No.: A21  
 Session: 2014-15 Parent Section: K2006  
 Details of Supervisor: Designation: AP  
 Name: Shabram Sharma Qualification: M.Tech-CSE  
 U ID: 14593 Research Experience: 0/1

SPECIALIZATION AREA: VANET Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

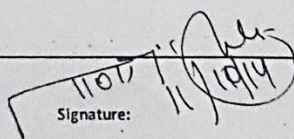
1. Secure Communication in VANET.
2. Authentication Scheme in VANET.
3. Attacks in VANET.

  
 Signature of Supervisor: 14593

PAC Remarks:

Student will work on different sized images, which is to be used at the time of authentication. Research paper will be published in future.

APPROVAL OF PAC CHAIRPERSON:

  
 Signature: 11/11/14

Date:

- \*Supervisor should finally encircle one topic out of three proposed topics and put up for a approval before Project Approval Committee (PAC)
- \*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
- \*One copy to be submitted to Supervisor.

## **ABSTRACT**

With the advancement in wireless communication technology and vehicle technology, exchanging of information, while travelling has become the most promising research field. Security is central to every major challenge, in one or the other aspect, the mobility model faces today. Proving the identity of one vehicle driver, during communication, to other vehicle drivers, along with message sharing is the main issue to cope with. To tackle this problem, efficient strategy that is adopted in VANET is to perform authentication of the vehicle drivers. The main objective of this research is to achieve the confidentiality of the message, along with the authentication of vehicle drivers. For this purpose, Steganography and Elliptic Curve Cryptography are used, where Driver License is used as Cover Image. Bit-level Extend and Dwindle (B-E&D) approach is used for hiding the message image of variable size behind the cover image. Mapping of Text Message bits with Cover Image decimal values is done, character by character, to generate the new image decimal values and is termed as E-O Toggle approach. For authentication and confidentiality, ECC is applied to the background image (user message image), before the embedding with the cover image.

# CERTIFICATE

This is to certify that Abhishek Kumar has completed M.Tech. Dissertation report titled “B-E&D and E-O Toggle Approach for Image and Text Embedding with ECC” under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation report has ever been submitted for any other degree or diploma.

The dissertation report is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech in Computer Science.

**Date:**

.....

***Ms. Shabnam Sharma***

(Asst. Professor, Department of  
Computer Science)

## **ACKNOWLEDGEMENT**

I feel great pleasure in submitting this report as the culmination of my guide's efforts. This required a very hard work, sincerity and devotion that I tried my best to put in my work and in turn gained a lot of knowledge and confidence from this analysis. I would like to acknowledge all those persons who help me for doing of this research.

I am deeply grateful to my mentor respected **Ms.Shabnam Sharma, Assistant Professor, CSE/IT, LPU** who has helped me in each and every step till begin till now. She has been a constant guiding force and source of illumination for me. It entirely goes to her credit that this work has attained its final shape. I would like to thank her for his valuable advice and guidance.

I also very grateful to our beloved parents deserve praise for the pain and sacrifices endured during my education also I thank to my classmates for had being there to help me out to integrate the new system that I have found here in LPU and the new life here in India, I really appreciate your contribution in my social and academic success equally. And I also thanks to all those persons who are directly or indirectly involved in completing my work.

**Thanks**

## **DECLARATION**

I declare that, this dissertation proposal entitled “B-E&D and E-O Toggle Approach for Image and Text Embedding with ECC” is original and has been submitted at Lovely Professional University in the partial fulfillment of the requirement for the award of the degree of M.Tech in Computer Science. The entire work is original and all ideas and references have been duly acknowledged. I declare this work is running successfully under the supervision of Ms. Shabnam Sharma, Assistant Professor, School of Information and Technology. It does not contain any work for the award of any other degree or diploma.

**Date:**

**Place: Lovely Professional University**

**Investigator: ABHISHEK KUMAR**

**Regn. No.: 11104802**

# TABLE OF CONTENTS

	TOPICS	PAGE NO.
1.	<b>INTRODUCTION</b>	1
	1.1 Introduction of VANET	1
	1.2 DSRC Technology	2
	1.3 VANET Architecture	4
	1.4 Security and Privacy	5
	1.4.1 Denial of Service (DOS) attack	6
	1.4.2 DDOS attack	6
	1.4.3 Sybil attack	6
	1.4.4 Timing attack	7
	1.4.5 Social attack	7
	1.4.6 Monitoring attack	7
	1.4.7 Application attack	7
	1.5 Steganography	8
	1.6 Elliptic Curve Cryptography (ECC)	8
	1.6.1 Elliptic Curve Groups over Real Numbers	9
	1.6.2 Properties of Elliptic Curves	9
	1.6.3 Advantages, Disadvantages and Applications of ECC	10
2.	<b>REVIEW OF LITERATURE</b>	12
3.	<b>PRESENT WORK</b>	16
	3.1 Problem Formulation	16
	3.2 Objectives of the Study	17
	3.3 Research Methodology	18
	3.3.1 Proposed algorithm	19
	3.4 Tool use: MATLAB	24
	3.4.1 Features of MATLAB	25

3.4.2	Uses of MATLAB	26
4.	<b>RESULTS AND DISCUSSIONS</b>	27
4.1	MSE and PSNR	27
4.2	Results at Sender Side	28
4.3	Result at Receiver Side	30
4.4	Graph representation of MSE, PSNR and Time Taken	32
4.5	Comparison between ECC and other asymmetric Encryption Technique	37
4.6	Timeline	38
5.	<b>CONCLUSION AND FUTURE SCOPE</b>	39
6.	<b>REFERENCES</b>	40
7.	<b>APPENDIX</b>	41
	List of Abbreviation	41
	Glossary of Term	43
	Meaning of Notation	45



# LIST OF TABLES

	<b>TABLE NAME</b>	<b>PAGE NO.</b>
1.1	Comparison of the Wireless Technologies	3
1.2	Application of DSRC	3
4.1	Values of MSE, PSNR, and TIME taken at Sender side	32
4.2	Values of MSE, PSNR, and TIME taken at Receiver side	34
4.3	Comparison of MSE, PSNR and Time value of different dimension's image	36
4.4	Comparison between key sizes of ECC and other asymmetric encryption method	37
4.5	Comparison of Signature sizes on long messages (e.g. 2000-bit)	37
4.6	Comparison between sizes of encrypted 100-bit messages	37
4.7	Timeline Gantt-Chart	38

# LIST OF FIGURES

	<b>FIGURE NAME</b>	<b>PAGE NO.</b>
1.1	Communication between RSU and Vehicles	2
1.2	Architecture model of VANET	5
3.1	Public-Key Cryptosystem: Authentication and Security	18
3.2	Flow-chart of Proposed work	19
3.3	Flow-Chart of Image Embedding	20
3.4	Operation done at Sender Side	21
3.5	Operation done at Receiver Side	21
3.6	Algorithm of Image Embedding	22
3.7	Algorithm of Text Embedding	22
3.8	Algorithm of Image Decoding	23
3.9	Algorithm of Text Decoding	24
4.1	Cover image of message and its histogram representation	28
4.2	Input Text Message Data	28
4.3	Message image and its histogram sending from sender	29
4.4	Encrypted image, its histogram, MSE and PSNR value	29
4.5	Embedded image, histogram, MSE and PSNR value	30
4.6	Cover image after separation, its histogram and MSE, PSNR value	31
4.7	Encrypted Message image after separation, histogram and MSE, PSNR value	31
4.8	Message Image, histogram, MSE and PSNR value, and Text Message data	32
4.9	Graph of MSE values at Sender side	33
4.10	Graph of PSNR values at Sender side	33
4.11	Graph of Time taken at Sender side	34
4.12	Graph of MSE values at Receiver side	34
4.13	Graph of PSNR values at Receiver Side	35
4.14	Graph of Time Taken at Receiver Side	35

4.15	Comparison graph of different dimension's images	36
4.16	Timeline report graph	38

# Chapter 1

## INTRODUCTION

---

### 1.1 Introduction of VANET

VANET (Vehicle Ad Hoc Network) is come from MANET (Mobile Ad Hoc Network). In MANET there is rapid development in wireless communications. It has made Inter-Vehicular Communications (IVC) and Road-Vehicle Communications (RVC), which has cause to birth new technology called, VANET. Despite of this fact, many differences exist between both of them.

1. The topology of VANET is changes quickly due to its high portability of vehicles.
2. Network fragmentation in VANET is frequently occurs.
3. The size network range is very small in VANET.
4. Redundancy of messages is limited in VANET both temporally and functionally.
5. Number of unique security challenges in VANET.

The primary point of VANET to give a high information rate and in the meantime minimize latency inside a relatively small communication zone. VANETs permit communicating with different vehicles and with the RSUs (Road Side Units). In VANET a communication connection exists between two vehicles is very short period of time, because of the fact that vehicles are go at a fast, more or less up to 200 km/h. Because of this it is hard to keep up any form of group membership. Protocols that depend on group membership are hard to actualize for a VANET. In VANET safety communication in a speed and secure way is the huge issue. In it Vehicles trade messages with one another like mindful of the street conditions, activity conditions, nearby data, and potential risky circumstances. When it is realized that there is a congested driving conditions, street conclusion or mishap ahead, a driver may securely evade the route and save time. Then again, a false message or a moment postponement can prompt risky circumstances, for example, crashes. Likewise, IEEE 1609.2 asymmetric Public Key Infrastructure with Elliptic Curve Digital Signature Algorithm (PKI/ECDSA) has been

proposed as default trial security system for VANET. VANET deals with DSRC (Dedicated Short Range Communication) innovation.

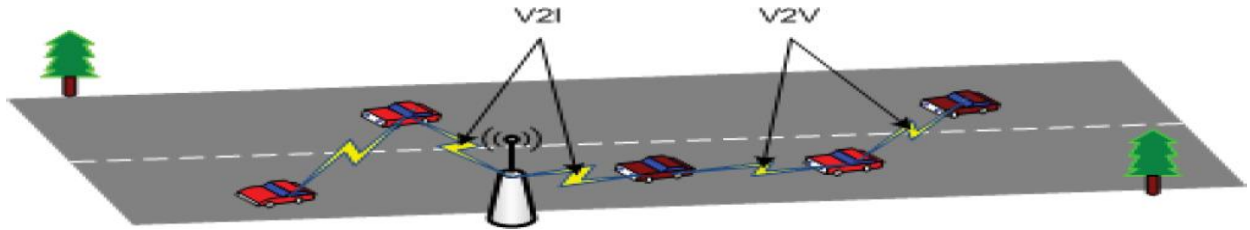


Fig. 1.1 Communication between RSU and Vehicles

Privacy and security are the most essential issues in VANET. In the first place, to gain support for the acceptance of a VANET the details of the driver must be saved, because public is not support VANET if driver's movement is recorded. Along these lines, keep up privacy of drivers is huge issue in VANET. Second, a VANET obliges a high level of security, means should not be conceivable to temper the messages in correspondence between vehicles. On the off chance that anyone can treating of security messages that would consequence of huge dangerous circumstance on street. In the event that strict efforts to establish safety are not convey in VANET communication then an attacker would have the capacity to inject false information into the system, that can be altered the stream of traffic and make chaos within the transportation system.

## 1.2 DSRC Technology

The Dedicated Short Range Communication (DSRC), effectively support vehicle-to-vehicle and vehicle-to-roadside security communication, which has known as Vehicle Safety Communication (VSC) technologies. VANET utilizes the DSRC technology to join the vehicle with the current infrastructure. It is also called WAVE (Wireless Access in Vehicular Environments). It is a short to medium range communication services and it gives a high information exchange rates. It supports both public safety and private operations from vehicle-to-vehicle and vehicle-to-roadside communications. It has small communication zones. DSRC works on 5.9 GHz frequency band. DSRC is in based on IEEE 802.11a standard and IEEE 1609 working group is being standardized as IEEE 802.11p for special vehicular

communication. It normally gives 6 to 27 Mbps data rate more than 1000 m communication range.

Table 1.1: Comparison of the Wireless Technologies

	<b>DSRC</b>	<b>Cellular</b>	<b>Satellite</b>
<b>Range</b>	100 – 1000 meters	Kilometers	Thousands of Kilometers
<b>Latency</b>	200 $\mu$ s	1.5 to 3.5 s	10 to 60 s
<b>Cost</b>	None	Expensive	Very Expensive

DSRC supports various different system protocols for interoperability of gaining widespread adoption. DSRC supports the TCP/IP so the most part of the traditional Internet applications are available in the VANET. The utilization of DSRC in remote technology now a day:

Table 1.2 Application of DSRC (Nurain Izzati Shuhaimi, 2012)

<b>Class</b>	<b>Description</b>
Vehicle-to-Vehicle application	Transmit messages from one vehicle to another.
Vehicle-to/from- infrastructure	Transmit messages either to or from vehicle to a road side unit (RSU).
Vehicle-to-home	Vehicle is parked at the driver's residence for purposes such as transferring data to the vehicle.
Routing based	Used when the intended recipient is greater than one-hop away.

Two types of DSRC devices are utilized for communication as a part of the VANET: an On-Board Unit (OBU) and a Road Side Unit (RSU). OBU which is a transceiver mounted inside a vehicle alongside a computational devices. OBU connected with omni-directional antenna which is utilized to get the wireless channel. Furthermore there is sensor on every vehicle to give the input to the OBU about the local condition of vehicle.

Second, RSU are stationary devices that are mounted road side. It is similar to OBU, also it has a transceiver, antenna, processor, and sensors. The main function of RSU's are to provide services to the vehicles on the road.

DSRC composed of public safety and non-public safety applications.

How vehicular network work;

- i) A router called as RSU where it connects the vehicular on the road with other network devices, called Base Station.
- ii) Each vehicle has OBU, where it connects the vehicle with RSU via DSRC radio.
- iii) Each vehicle has Tamper Proof Devices (TPD), where it holds vehicle secrets such as driver's identity, speed, acceleration, route etc.

DSRC application can be categorized as safety and non-safety applications, and the application message of DSRC may be either occasion driven or periodic. The occasion driven messages are those messages which are sent when a certain event happens. For example, if any crash is happened on street then all vehicles close to that impact are exchanged that event message to further vehicles. On the other hand, periodic messages are more than once transmitted at a particular interval, for example, a street conditions, status of traffic lights.

### **1.3 VANET Architecture**

VANET is Intelligent Transportation Systems (ITS) which give numerous facilities to the drivers. The structural planning of VANET is less complicated, it is the same as tree structure. The architecture comprises of Central trusted Authority (TA) at the root, trailed by state level trusted Authorities (STA) thereunder, and a group of city level trusted Authorities (CTA) under every STA. Ultimately, under every CTA there are several of RSUs and a group of vehicles that moving on a street. Likewise of it, an OBU or RSU is equipped with private and public key, together with a shared key which are given by its immediate higher authority. The function of TA is, it will distribute both public and private keys, together with the certificate to STAs. A STA plays the function of key distributor for CTA and comparatively, CTA will distribute the key and short certificates back to OBU or RSUs. Other than OBU, every vehicle has TPD with a specific end goal to store these different keys, Process that takes place is; a vehicle will get a short certificate at the time of authentication by CTA by means of

the corresponding RSU for inter-vehicle communication. Note that, numerous RSU, under a CTA are assembled together such that their identities have a common two bit prefix as group identifier.

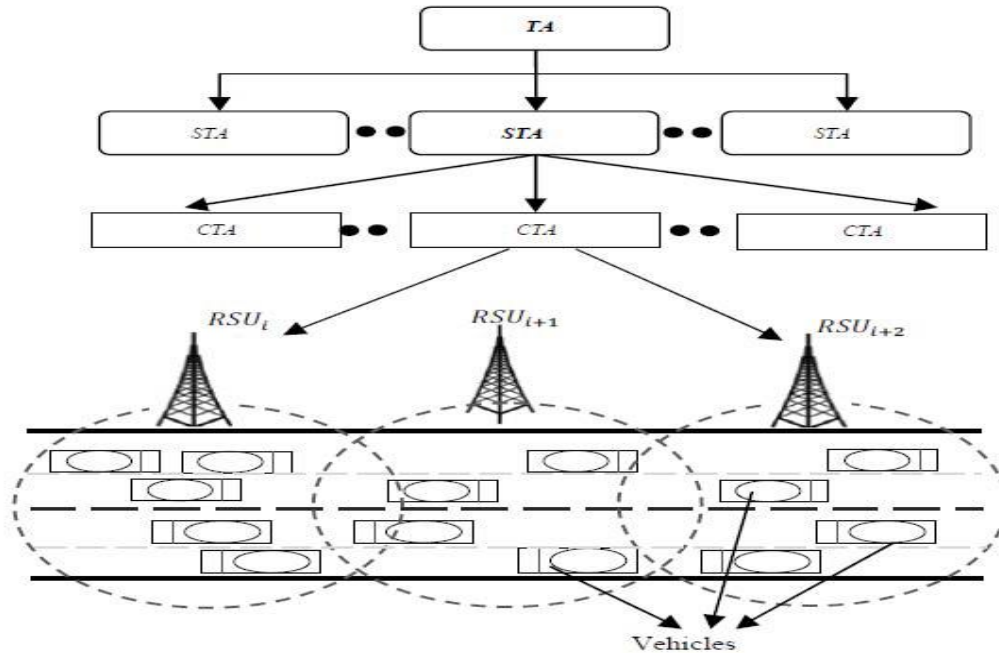


Fig. 1.2 Architecture model of VANET (Nurain Izzati Shuhaimi, 2012)

## 1.4 Security and Privacy

Securing vehicle-to-vehicle and vehicle-to-roadside communication is most important thing in VANET deployment. The system must ensure that the transmission comes from a trusted source, and that transmission has not been tampered by any intruder. For example, if any vehicle send message about road condition i.e. “Road is damaged! Go slowly” but some intruder temper that message with “road is in good condition, go with you speed” then another vehicle can don’t know about road condition and it create difficulties for that vehicle’s driver. Privacy and anonymity are also major issues in VANET. For example, if any one send the information about their vehicle current location, speed and another valuable information to another vehicle, but at the same time if any intruder also able to access those messages then he easily misguide or harm that vehicle.

Due to the large number of independent network members and the presence of the human factor, it is highly probability that misbehavior will arise in this network. Some users use it for only own beneficial or to create some hazardous situation on road. They do many types of



attacks on it and try to damage this life saving architecture. Many types of attacks are done by some illegal people on this mechanism. The objective of those attacks is to create problems for other users in the network or to prevent communication. In it different types of attacks, their threat level, and attacks priority.

The proposed classes for attacks are:

- i) Denial of service (DOS) attack
- ii) Distributed DOS (DDOS) attack
- iii) Sybil Attack
- iv) Timing attack
- v) Social attack
- vi) Monitoring attack
- vii) Application attack

#### **1.4.1 Denial of Service (DOS) attack**

It is a standout amongst the most genuine level attacks in vehicular system. In DOS attack, attacker jams the primary communication medium and system is no more available to genuine customers. The key purpose of DOS attacker is to keep the genuine customers to get to the system services. It additionally extends the danger to the driver, in the event that it needs to rely on upon the application's data.

#### **1.4.2 DDOS attack**

For this circumstance attacker launch attack from particular regions. They may use distinctive time slots for sending the messages. Nature of the messages and time slot may be shifted from vehicle to vehicle of the attacker. The purpose of the attacks is same i.e. to down the system.

#### **1.4.3 Sybil attack**

This attack happens when an attacker makes vast number of pseudonymous or provides illusion and claims or acts like it is more than a hundred vehicles, to tell different vehicles that there is jam ahead, and force them to take alternate way to go.

#### **1.4.4 Timing attack**

This is new type of attack in which attacker's main target is to include eventually some time slot in original message and create delay in original message. Attacks don't bother the other substance of message, just create delay in the message and these messages are gotten after it obliges time.

#### **1.4.5 Social attack**

All unmoral messages (social attack) are lie on this class. It is kind of messages is to indirectly create problem in the network. Legitimate users show angry behavior when they receive such kind message.

#### **1.4.6 Monitoring attacks**

In this attack, the attacker just monitor the whole network, listen the communication between V2V and V2I. If they find any related information then pass this information to concern person.

#### **1.4.7 Application attacks**

In this kind of attack, primary concern of the attacker is to change substance of these applications and utilization it for their own particular advantages. Two types of application-attacks in VANET: Safety and Non-Safety. Warning messages is important messages that are utilized as a part of safety application, e.g. Attacker B gets one notice message "Work Zone Warning" from close-by vehicle. So he changes the substance of the message and sends this message "Street is Clear" to other vehicle C. Non safety application is related with client's comfort during their journey, e.g. Valid client A get data "Parking is available" from Road side unit (RSU) close to the shopping center. So he sends this message to other vehicle B. This vehicle B is attacker and now he adjusts this message to this message "No parking is available" and passes this message to other vehicle C.

## **1.5 Steganography**

Steganography is the art and science of concealing information during communication. Purpose of steganography is conceal the messages from eavesdropper. In the past, peoples was used tattoos or invisible ink to sending the messages i.e. also a part of steganography, but in today computer and network technology provide easy to use steganography in communication channels.

Information hiding process in steganography starts by identifying the redundant bits of cover medium. After that these redundant bits are replaced with data from the hidden message. The modern steganography's goal is to keep undetectable by eavesdropper. Steganography is separate and distinct from cryptography, because In cryptography we completely change the bits with another bits which are coming after using some keys or encryption algorithms but in Steganography we only replace some bits of cover medium with the hidden message bits, so our cover message data cannot distort or not visible to eavesdropper.

Three different aspects are available in information-hiding systems: capacity, security and robustness. Capacity refers to the amount of information that can going to conceal into the cover information, security refers to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

## **1.6 Elliptic Curve Cryptography (ECC)**

Elliptic curve cryptography is a method of encoding data so only specific user can able to decode that data. ECC is based on the Elliptic curve. Points on an elliptic curve is used to encrypt and decrypt information. Victor Miller of IBM and Neal Koblitz of the University of Washington first proposed ECC, in the 1980s. ECC has been adopted by many companies or technology for providing security on the information. ECC has been standardized by the American National Standards Institute, the National Institute of Standards and Technology and the Federal Information Processing Standard.

## 1.6.1 Elliptic Curve Groups over Real Numbers

An elliptic curve for real numbers are defined as set of points  $(x, y)$ , that satisfy the elliptic curve equation, i.e.  $y^2 = x^3 + ax + b$ , where  $x, y, a$  and  $b$  are real numbers. If  $x^3 + ax + b$  is not contain any repeated factors, or  $4a^3 + 27b^2$  is not equal to 0, then elliptic curve equation  $y^2 = x^3 + ax + b$  used to create a group of points.

## 1.6.2 Properties of Elliptic Curves

There are some useful properties of elliptic curve are used in cryptography:

- i. Point Addition
- ii. Point Doubling
- iii. Scalar multiplication

### i. Point Addition:

When  $P = (x_p, y_p)$  and  $Q = (x_q, y_q)$  are not negative of each other,

$P + Q = R$  where

$$s = \frac{(y_p - y_q)}{(x_p - x_q)}$$

$$x_r = s^2 - x_p - x_q$$

$$y_r = -y_p + s(x_p - x_r)$$

Note that  $s$  is the slope of the line through  $P$  and  $Q$ .

### ii. Point doubling:

When  $y_p$  is not 0,

$2P = R$  where

$$s = (3x_p^2 + a) / (2y_p)$$

$$x_r = s^2 - 2x_p \text{ and } y_r = -y_p + s(x_p - x_r)$$

here  $a$  is the one of parameters chosen from the elliptic curve and  $s$  is the tangent on the  $P$ .

### iii. Scalar multiplication:

Scalar multiplication is the dominant computation part of ECC. It computes  $kP$  by adding point  $P$  copies together of the  $K$  times, such as  $Q = k \times P = (P + P + \dots + P)((k - 1) \text{ addition})$ .

### 1.6.3 Advantages, Disadvantages and Applications of ECC

#### Advantages:

- **Size of the key:** The size of the key required for encryption and digital signatures is surely far less than other systems.
- **Less time for encryption.**
- None of the currently known algorithms for the solution of the DL problem can be applied. The use of brute force attack on ECC takes a lot longer time to be successful.
- Any cryptographic scheme/protocol based on discrete logarithms can be easily converted to elliptic curve form.
- If the order of the fixed point F is an n-bit prime, then computing k from  $k \cdot F$  and F takes roughly  $2^{(n/2)}$  operations.

#### Disadvantages:

- ECC utilizes elliptic curves, generators and finite fields, and points of curve, which can lead to more complex calculations that could strain an embedded processor.
- This can be circumvented with lookup tables for elliptic curves, but this can eat up valuable resources on handheld and portable devices.
- The field has not been tested widely, compared to other fields.
- Probability of future discovery of sub exponential attack. A successful discovery of an attack on the system can weaken the immunity of the system.
- ECC systems are slower than RSA in public key operations. So in applications requiring vast public key encryptions, the system is not desirable.

#### Applications:

**Applications involving Constrained Channels:** Constrained channels are those, which are limited in memory, processing and other resources. In such situations, following advantages of ECC are surely more helpful.

- Shorter keys

- Shorter signatures
- Shorter certificates
- Simple generation of key pair

## CHAPTER 2

# REVIEW OF LITERATURE

---

In this chapter we put the all work done by different researcher in a VANET security, authentication of messages and steganography techniques. Previous work conducted for preserving the privacy and techniques that were used for efficient and scalable group communication are discussed in this section.

(Baber Aslam, 2009) Proposed Distributed Certificate Architecture for Vehicular Ad hoc Network. On receiving the request from user, Certificates were issued to vehicle drivers by Trusted Third Party. In this approach, eavesdropper would not be able to get the information about any authorized vehicle driver, because information about vehicle drivers was stored at TTP. Due to restricted nature of that issued certificate, revocation process would be initiated if maximum time limit is achieved or user has moved out from coverage area.

(Chin-Chen Chang, 2009), proposed an information embedding scheme, which is utilized to achieves low computation expense and high concealing capacity. They utilizes an exclusive operation to cover secret information that strategy is additionally save calculation expenses associated with the embedding procedure. Since secret information is inserting in segment-wise, the distribution of wet pixels lead more segments to which conceal the secret information. They utilized random number generator or permuting selected pixels of interest for selecting wet pixels. To locate the longest row of consecutive wet pixels from picture they utilize raster scanning method.

(Asif Ali Wagan, VANET Security Framework for Trusted Grouping using TPM hardware, 2010) Used Trusted Platform Module and Hybrid Message Dissemination scheme for faster and secure communication. Framework suggested in this paper consists of Hardware Entity (TPM Chip), Group Entity and Group Communication. The main motive of research was to achieve trust among vehicles to create trusted group. When new group formation was carried out, Asymmetric encryption technique was used and group key was generated and distributed

among group members. Further, the author has suggested, the use of asymmetric key cryptography for encrypting periodic messages and symmetric key cryptography was suggested for event driven messages.

(Ghassan Samara, 2012) Proposed the usage of VPKI as an issue, where each node will have a public/private key. Any Vehicles need to send safety messages to other then it signs that with it specific private key and incorporates the Certificate Authority. In the meantime using of VPKI as an issue of VANET having a couple of troubles, in the same route as support of an attacker must be repudiated. Transport of CRL is the most well-known methodology to disavow the support that contains all repudiated statements. This methodology has similarly a couple of disservices: First, CRLs can be long as a result of the tremendous number of vehicles and their high flexibility. Second, the sort lifetime of affirmations still make powerlessness and last is that there is no foundation for the CRL.

(F. Amounas, 2012) Proposed an algorithm based on Elliptic Curve Cryptography and generated the rational points on elliptic curve. Data sequence was then generated using ECC and populated in the matrix. Right Shift was performed on the elements of the matrix  $X_m$  and stored in new matrix  $X_{new}$ . Cipher Text was produced by pairing the element of the matrix,  $X_{new}$  and point generated from random number  $R_n$ .

(U. Rizwan, 2012) Categorized the methods of Steganography in two broad categories: Spatial Domain approach and Frequency Domain approach. In former approach, data was embedded by modifying the gray level of few pixels of the cover image, which can be easily detected by performing computer analysis. In latter approach, one of the DFT, DCT and DWT can used to embed the data in the coefficients of cover image. But, for hiding large amount of data, Frequency Domain was not suitable. The author has produced an analysis report on MSE, PSNR and SSIM indices for different variations of Least Significant Bit Steganography methods including Odd Memory Location, Even Memory Location, Prime number location, Minimum Gray level, Maximum gray level, Spiral Matrix Location and Magic Square Location.



(Nurain Izzati Shuhaimi, 2012) Proposed Identity based Encryption scheme, in which private and public key were not generated at the same time, unlike PKI. In the proposed scheme, Trusted Third Party played the role of arbitrator. Upon the reception of user request at Trusted Third Party (TTP), public key was then generated and shared with the sender. At sender site, message was encrypted with public key and sent to Receiver. At receiver site, request for private key was sent to TTP and decryption process was initiated, to obtain the plain text. There is no role of Certification Authority for issuing the certificates.

(Vijay Kumar Sharma, 2012) Proposed steganography algorithm, which has represented the cover image pixel value into RGB format of 24 bit. Text message of user was then represented in eight bit format. Eight Most Significant Bits of Blue intensity color of cover image pixel values were replaced by eight bits of text message. After replacing, new pixel values were stored in matrix for the generation of new image, after embedding of text message. Due to low visual perception of blue component, blue color was selected, for the replacement with text message bits. But, this algorithm, also suffered from distortion.

(Chetan V.S, 2013) Proposed an efficient technique of hiding message image behind the cover image. Vehicle License Plate was used as cover image as well as proved the authenticity of the vehicle driver to other vehicle drivers, during communication. For Privacy preservation, symmetric encryption technique Bilinear Cryptography was used. This algorithm was suited for image embedding, where the size of cover image and message image must be same.

(Aditya Sinha, 2014) Proposed an efficient method to defend against DOS attacks i.e. Queue Limiting Algorithm (QLA). According to this method vehicle in a network has limited capacity of message receiving, without having any security risk. In this the capacity of receiving messages is limited at the receiver side, so OBU will perform its task quite easily. Message priorities is also checked by communication channel. DSCRC spectrum is divided into seven 10-MHz channels. In it channel number 178, which is generally restricted to safety communication was a highest priority, and the channels 174, 176, 180, or 182 are the 2nd highest priorities.

(Manish Kumar Soni, 2014) Proposed advancement the security of area based directing which is viability and upgraded security. It can be shortened form of two angles: Routing message assurance system and Node assessment instrument. In this information exchange among every two vehicles is marked by the sender and the mark prerequisites to be built no issue which hub got it. At the point when any vehicle makes an impression on any far away vehicle. It will get the position data of the target vehicle and after it is bundled together with the sending message, steered by the position-based convention ingeniously to the terminus. For the insurance of steering message, a mark checked plan is utilized to accomplish end-to-end validation and respectability of the information.

## **CHAPTER 3**

# **PRESENT WORK**

---

In this chapter, discuss about the problem formulation, objectives and Methodology of the research. In problem formulation, defined how to find the problem in given area and what type of process or techniques are going to use for solving that problem. In objective section, discuss about the objective of research, what is the benefit of this research? What type of problems are overcome by implementing this proposed techniques? In Methodology section, discuss about the how to solve that problem. What type of methodology are going to use for getting the suitable results.

### **3.1 Problem Formulation**

VANET, is a technology which provide the communication between vehicles. Using VANET, vehicles are easily exchange the data which is useful for driver. So, security on those data is very concern thing. First, anybody don't want to see their data with any third person, who are not concerned with that data. Second, they don't want to alter their data by any person in between traveling on the network. In VANET it is more conscious thing because if anybody change the data in between, then those data is very harmful for driver or any other person who are on the street. Third, the authentication of driver or vehicles is the most important part in VANET, because if driver does not authenticate then receiver doesn't know about who is the sender or that sender is legitimate or not.

So achieving above security on message transferring between two vehicles we are going to used two techniques: first is Steganography and second is Asymmetric key encryption technique. Steganography is used for achieving the secrecy of the data and Asymmetric Key encryption technique is used for security of the data. There are many types of asymmetric encryption methods are available but we use Elliptic Curve Cryptography technique, because it is very fast as compare to another encryption method.

There is one research paper (i.e. already ready discussed in review of literature section) on which researchers are also try to solve that above problem but they are not able to embedding

two different size of images. They always use same size of images for data secrecy. They use symmetric encryption technique for securing the data, and for authentication of data they used vehicle license plate image as a cover image of data hiding. Receiver only identify the sender by looking the cover image but there is chance to malicious driver also used another vehicle's license plate image for cover image of message and show at receiver that he is a legitimate user. So I am going to overcome these problems on this research.

### **3.2 Objectives of the Study**

There are two objectives of this research:

1. Text messages and Images of variable sizes are embedded to achieve data secrecy during communication using Steganography.
2. Asymmetric ECC technique is used for authenticating the message.

The main objective of this research is easily embedding two variable size of images with each other, and also distortion on cover image could not occurred by embedding two images. The Vehicle license plate (VLP) image is going to use for the cover image of message data. So if any third party is going to check data they only see the image of VLP. VLP is also help for authentication of sender driver of vehicles. The steganography technique is used to secrecy of data.

Second objective of this research is, if sender want to send some text data to the destination vehicle then there is facility to sending the text data. Text data is also sending to the destination by embedding with message image. So if no one can know about that there is any text data is also sending by sender.

Third objective of this research is, security of message data and authentication of driver or sender vehicle. For achieving these objective asymmetric encryption technique is used. There is many asymmetric techniques are available but we used Elliptic Curve Cryptography. ECC is very fast as compared to another asymmetric techniques. It provide more security using small key as compare to RSA. For authentication of message VLP is used but there is chance that another malicious user also use the VLP of legitimate user and represent itself behalf of that user. So ECC can also provide authentication because it is asymmetric key encryption technique, in it we encrypt messages two times, first encrypt that message by sender using its own private key and again encrypt that encrypted data using public key of receiver vehicle. So

only particular user could be able to decrypt that message using its own private key and again decrypt that message by only using sender public key.

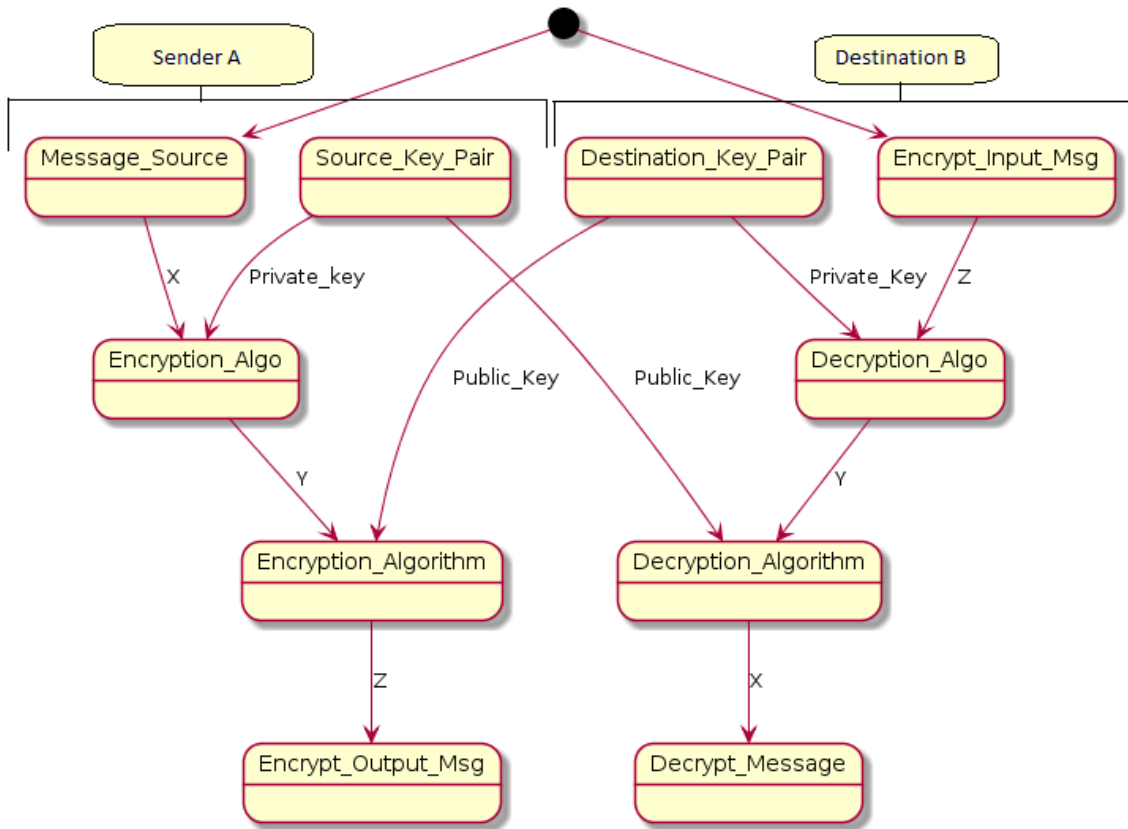


Fig. 3.1 Public-Key Cryptosystem: Authentication and Security

### 3.3 Research Methodology

In steganography, various techniques of hiding images or text messages behind the cover image are available. Least Significant Bit (LSB) is the most common technique of hiding data. But, the main drawback of LSB is that, it leads to the distortion of cover image. A new technique of hiding data is proposed, in which cover image will not distort. Algorithm for Image Embedding, Text Embedding, Image Decoding, and Text Decoding are described in subsequent section. Bit-level Extend and Dwindle (B-E&D) approach is implemented in Image Embedding Algorithm. For authenticity and secrecy of data, Elliptic Curve Cryptography is used for encryption and decryption.

### 3.3.1 Proposed Algorithm

#### At the Sender Site:

*Step1:* Input the background image BI, cover image CI, and text message  $TU^j$ .

*Step2:* If user wants to send text message, the approach “E-O Toggle” is mentioned in “*Algorithm for Text Embedding*”.

*Step3:* Encrypt, newly generated  $N_i$  image from matrix  $O_1$ , using ECC Encryption Technique.

*Step4:* Embed the Encrypted Image  $N_i$ , with Cover Image CI, by following “B-E&D approach” specified in “*Algorithm for Image Embedding*”, by considering  $N_i$  as background image for future operations.

*Step5:* Send that embedded data to the destination.

#### Flow-diagram of sending messages:

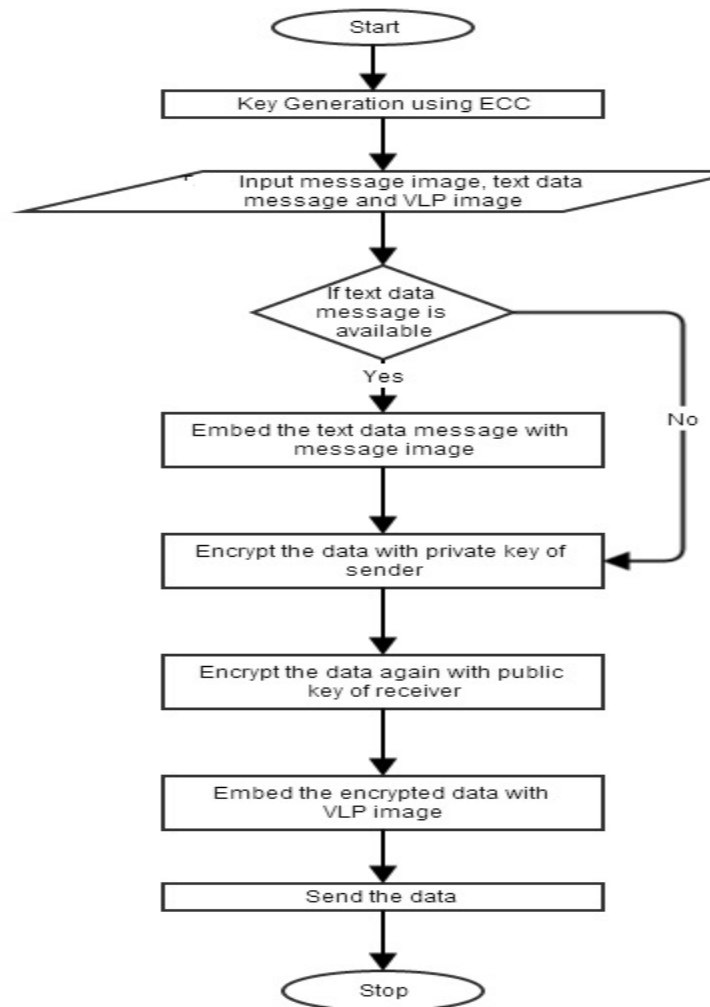


Fig. 3.2 Flow-chart of proposed work

### Flow-diagram of Image embedding:

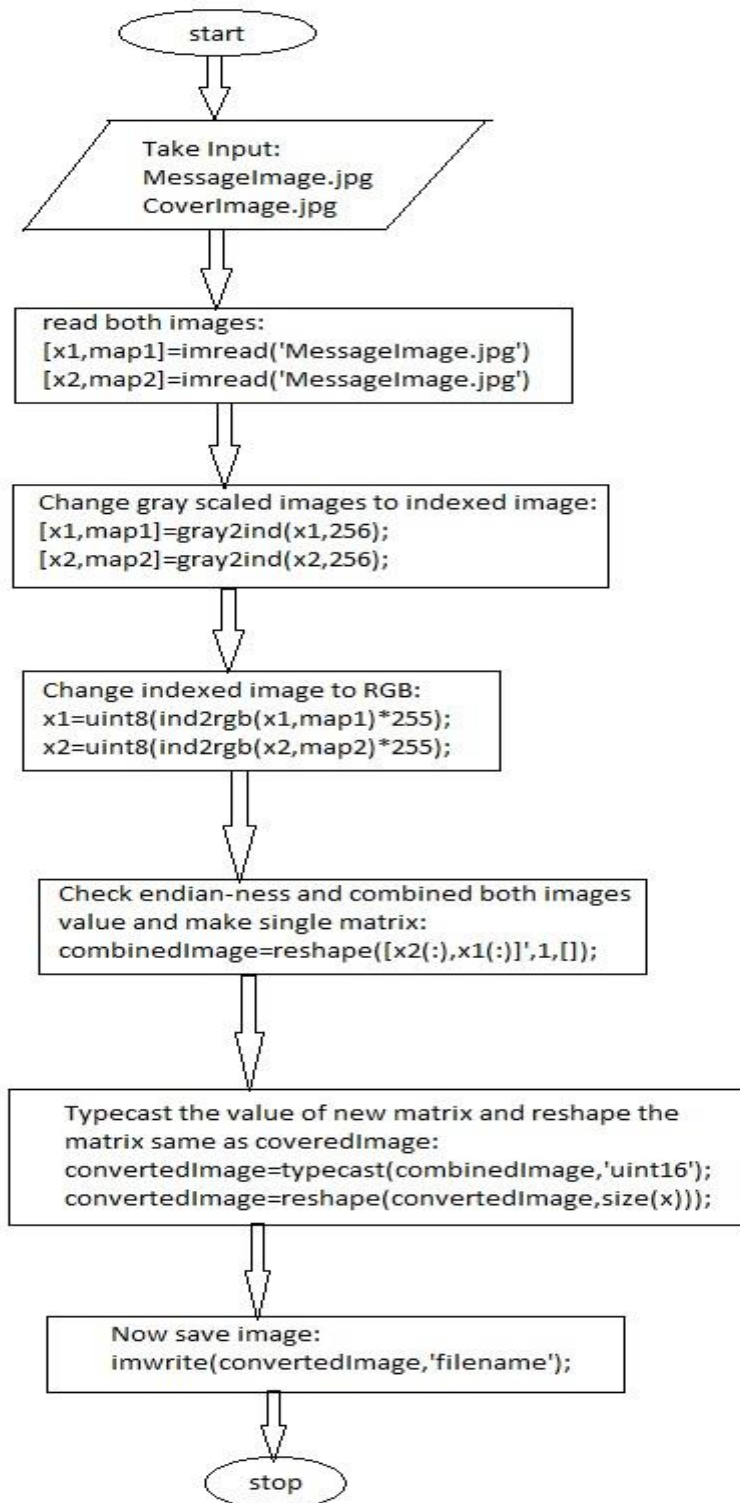


Fig. 3.3 Flow-Chart of Image Embedding

### Sequence Diagram of Proposed Work:

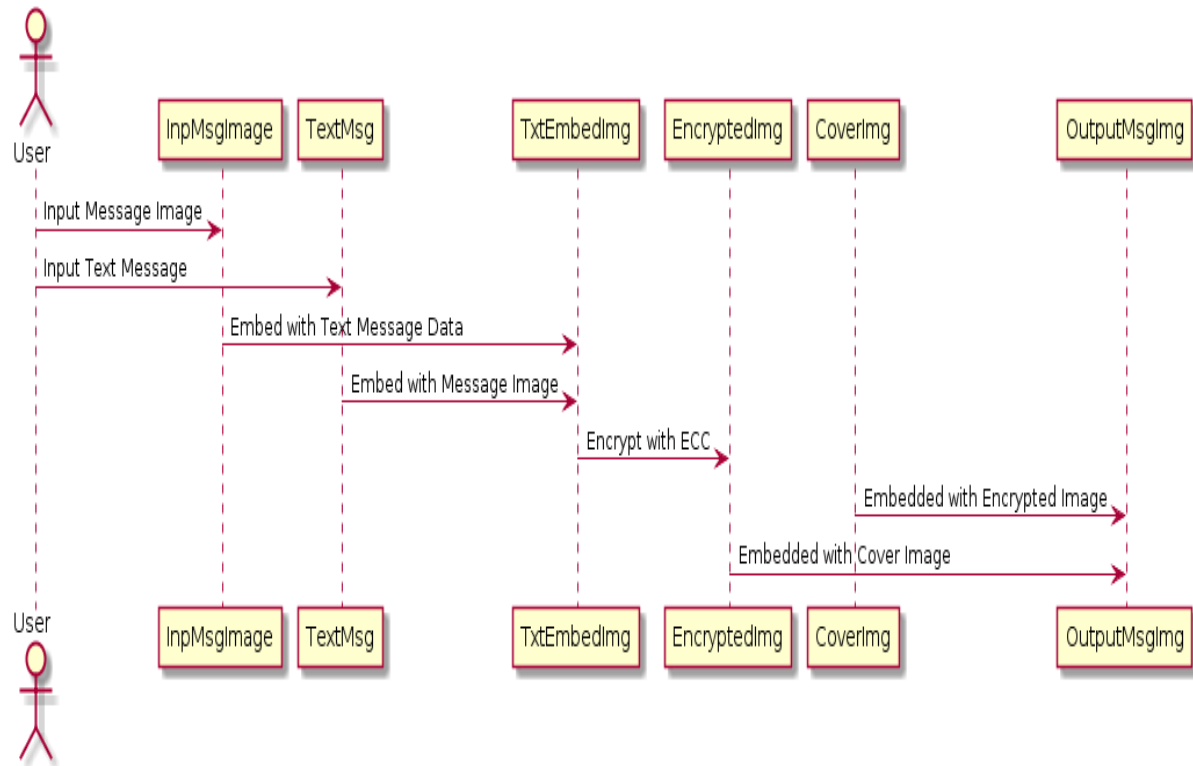


Fig. 3.4 Operation done at Sender Side

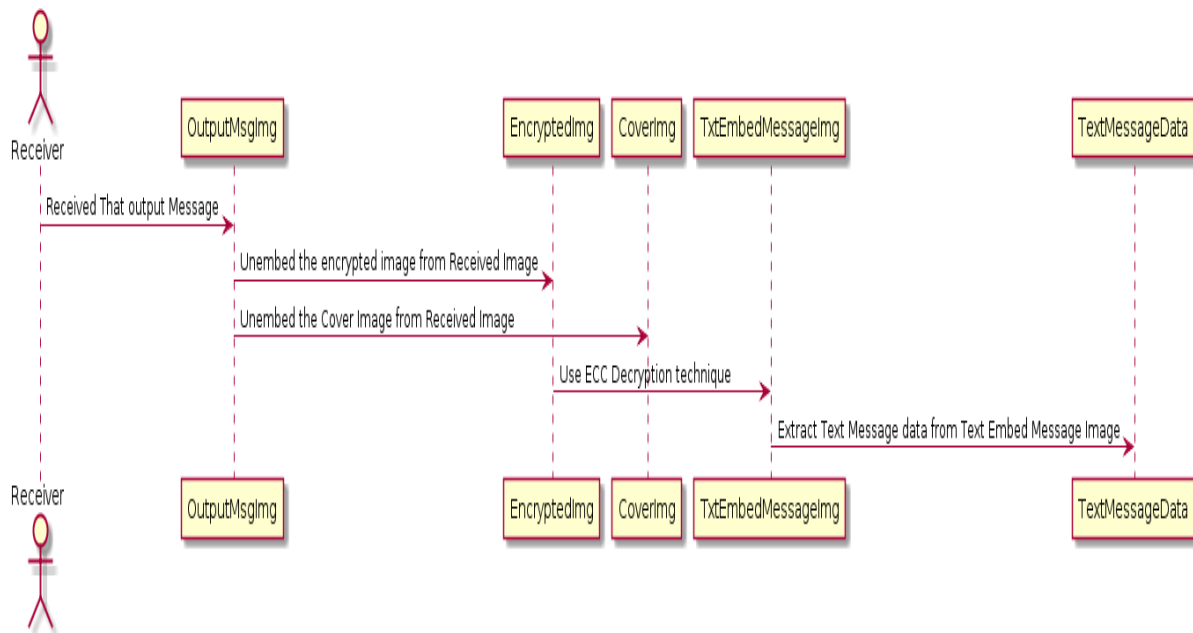


Fig. 3.5 Operation done at Receiver Side



---

**Algorithm 1: Image\_Embedding()**

---

Data: Input Background Image (BI) and Cover Image (CI)  
Result: New Image,  $S_1$   
**Begin**

- 1 Convert BI and CI to Matrices  $X_1$  and  $X_2$  respectively.
- 2 Change the indices of BI and CI into RGB format.
- 3 Create new matrix  $X_3$  and populate the matrix by selecting values from BI and CI, alternatively.
- 4 Typecast values of matrix  $X_3$  to unsigned integer of 16 bit.
- 5 Create the new image,  $S_1$  from  $X_3$ , using bits of CI only.

**End**

---

Fig 3.6: Algorithm of Image Embedding

---

**Algorithm 2: Text\_Embedding()**

---

Data: Input Text Message,  $TU_j^i$  and Cover Image, CI.  
Result: New Image,  $N_i$ , Output Matrix  $O_1$ .  
**Begin**

- 1 Convert the ASCII value of every character of  $TU_j^i$  into 8-bit binary representation and store it in matrix  $Y_b = \{b_0, b_1, b_2, \dots, b_n\}$ .
- 2 Create the matrix  $Y_1$  from CI.
- 3 Maximum elements can store in  $Y_b$  is represented by  $n$ , where  $n = \text{numel}(Y_b)$
- 4 **For**  $b=0$  to  $n$  do
- 5     Set  $x=Y_b(n)$  and  $z=Y_1(n)$
- 6     **If**  $((x==0) \ \&\& \ (z\%2!=0))$  then
- 7         |     Set  $z=z-1$  and store it in  $O_1$ .
- 8     **Else if**  $((x==1) \ \&\& \ (z\%2==0))$  then
- 9         |     Set  $z=z+1$  and store it in  $O_1$ .
- 10     **End if**
- 11     **End For**
- 12 Plot the new image  $N_i$ , from newly generated matrix  $O_1$ .

**End**

---

Fig 3.7: Algorithm of Text Embedding

**At the Receiver Site:**

*Step1:* Upon the reception of data, decoding process will be initiated by the receiver.

*Step2:* Decode the background image from received image, by executing the steps mentioned in “*Algorithm for Image Decoding*”.

*Step3:* Decrypt that image using ECC technique.

*Step4:* Recover text message from image by applying “*Algorithm for Text Decoding*”.

---

**Algorithm 3: Image\_Decoding()**

---

Data: Input Received Image (RI).

Result: Matrices  $X_5$  and  $X_6$ , Received Background Image (RBI), Received Cover Image(RCI).

**Begin**

```
1   Convert the RI into matrix  $X_4$ .
2   Typecast the matrix  $X_4$  values into unsigned
    integer 8 bit format, where matrix values are
    represented as  $D=\{d_0,d_1,d_2,\dots,d_n\}$ .
3   Set  $j=0$ 
4   Set  $k=0$ 
5   For  $h=0$  to  $n$  do
6       Set  $g=D_h$ 
7       If  $(h\%2==0)$  then
8           Set  $X_5[j]=g$ ;
9            $j++$ ;
10          Else
11              Set  $X_6[k]=g$ ;
12               $k++$ ;
13          End if
14      End for
15      Generate images from newly created matrices,
         $X_5$  and  $X_6$ .
16      One of them is Cover Image and another is
        Background Image.
```

**End**

---

Fig 3.8: Algorithm of Image Decoding

---

**Algorithm 4: Text\_Decoding()**

---

Data: Input Received Image (RI), size of text.  
Result: Original text message,  $TU_j$ .

```
Begin
1  Convert the RI into decimal values and store
   it in matrix  $XM_7$ , where
    $XM_7 = \{d_0, d_1, d_2, \dots, d_n\}$ .
2  Set  $k=0$ 
3  For  $j=0$  to  $n$  do
4  |   Set  $s = XM_j \% 2$ 
5  |   Set  $X_{temp}[k] = s$ 
6  |   Set  $k = k + 1$ 
7  |   If  $(k == 8)$  then
8  |   |   Set  $k = 0$ 
9  |   |   Convert all 8-bit binary values, stored in
   |   |    $X_{temp}$  into decimal notation in matrix  $X_8$ .
10 |   End if
11 End For
12 Convert all ASCII values (decimal notation) into
   characters to produce the original text message,
    $TU_j$ .
13 End
```

---

Fig 3.9: Algorithm of Text Decoding

### 3.4 Tool use: MATLAB

We are using MATLAB tool for implementing the above proposed algorithms. MATLAB is a programming dialect created by MathWorks. It began as an issue programming dialect where direct polynomial math writing computer programs was simple. It can be run both under intelligent session and as an issue work.

MATLAB is a fourth-era high-level state language and intelligent environment for numerical reckoning, visualization, and programming. Utilizing MATLAB, we can examine information, create calculations, and make models and applications. It permits network controls, plotting of capacities and information, usage of calculations, formation of client interfaces, interfacing

with projects written in different language, including C, C++, Java, and FORTRAN, examine information, create calculations, and make models and applications.

MATLAB is utilized as a part of each aspect of computational math:

- ✓ Dealing with Matrices and Arrays
- ✓ 2-D and 3-D plotting and representation
- ✓ Linear Algebra
- ✓ Algebraic Equations
- ✓ Non-direct Functions
- ✓ Statistics
- ✓ Data Analysis
- ✓ Calculus and Differential Equations
- ✓ Numerical Calculations
- ✓ Integration
- ✓ Transforms
- ✓ Curve Fitting
- ✓ Various other Special Functions

### **3.4.1 Features of MATLAB**

- ✓ It is a high-level state language for numerical calculation, visualization and application improvement.
- ✓ It is additionally gives an intuitive environment to iterative investigation, outline and critical thinking.
- ✓ It gives boundless library of scientific capacities for direct variable based math, insights, Fourier investigation, sifting, advancement, numerical combination and explaining normal differential mathematical statements.
- ✓ It gives implicit design for envisioning information and apparatuses for making custom plots.
- ✓ MATLAB's customizing interface gives advancement devices for enhancing code quality and viability and augmenting execution.
- ✓ It gives devices to building applications with custom graphical interfaces.
- ✓ It gives capacities to coordinating MATLAB based calculations with outside applications and dialects, for example, C, Java, .NET and Microsoft Excel.

### **3.4.2 Uses of MATLAB**

- ✓ Signal Processing and Communications
- ✓ Image and Video Processing
- ✓ Control Systems
- ✓ Test and Measurement
- ✓ Computational Finance
- ✓ Computational Biology

## CHAPTER 4

# RESULTS AND DISCUSSIONS

---

In this chapter, discussed about the implementation of proposed methodology and outcomes after implementation. Discussed about the many phases which are occurred during implementation. All implementations are done through MATLAB. We used Image processing tool of MATLAB for embedding two images or text data with images. Results of the implementations are show through histograms and also calculated MSE and PSNR value of images. Time taken of implementation by different processes are also calculated.

### 4.1 MSE and PSNR

MSE and PSNR are two error measurements used to analyze picture compression quality. The MSE represents to the cumulative squared error between the compressed/reconstructed image and the original image. MSE is a risk function, related with the expected value of the squared error loss or quadratic loss. The lower estimation value of MSE, represents lower error.

PSNR represents to a measure of the peak error. It is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is generally expressed in terms of the logarithmic decibel scale. PSNR is most ordinarily used to measure the quality of recreation of loss compression codecs. PSNR is characterized by means of the MSE.

To compute MSE and PSNR, the following equation are used:

$$MSE = \frac{\sum_{M,N} [I_1(m, n) - I_2(m, n)]^2}{M * N}$$

In the above equation, M and N are the number of rows and columns in the input images, respectively. Then PSNR computes using following equation:

$$PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right)$$

## 4.2 Results at Sender Side

When any driver want to communicate with another vehicle then he used its own VLP image as a cover image of message.

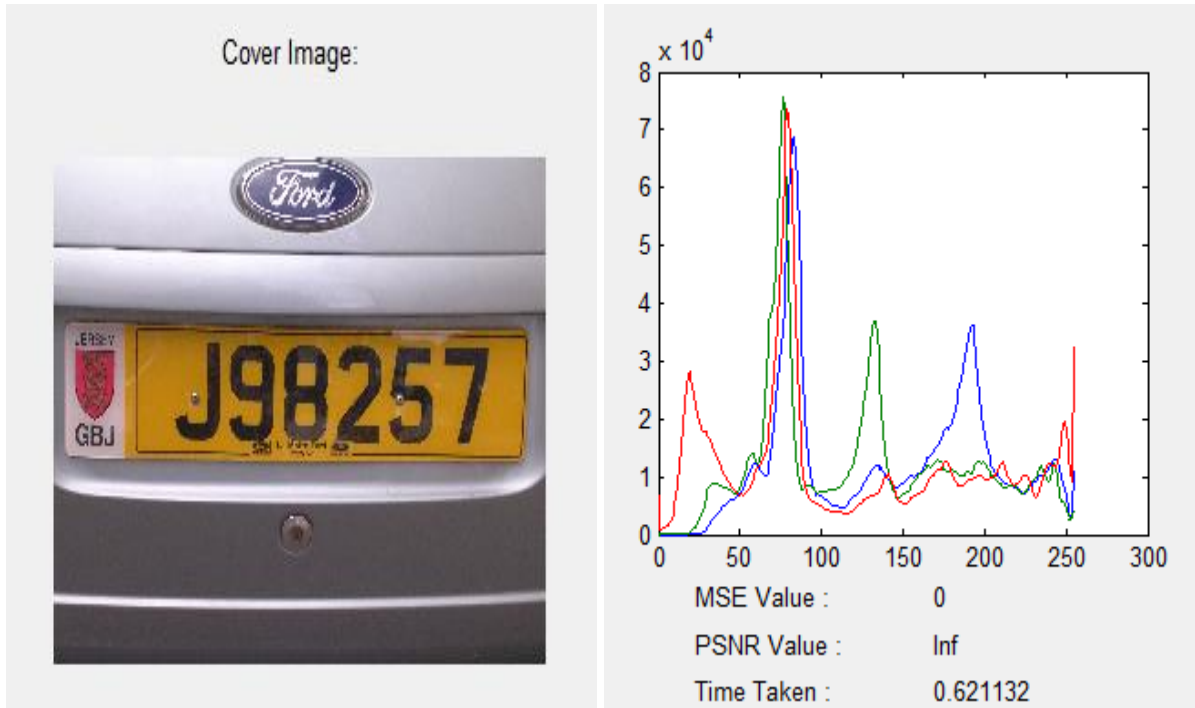


Fig. 4.1 Cover image of message and its histogram representation

If sender vehicle want to send some text data then he also give input some text data to the message.

Enter your Text Message :

Fig. 4.2 Input Text message Data.

Then Sender must enter the message image which vehicle's driver want to send to another vehicle.

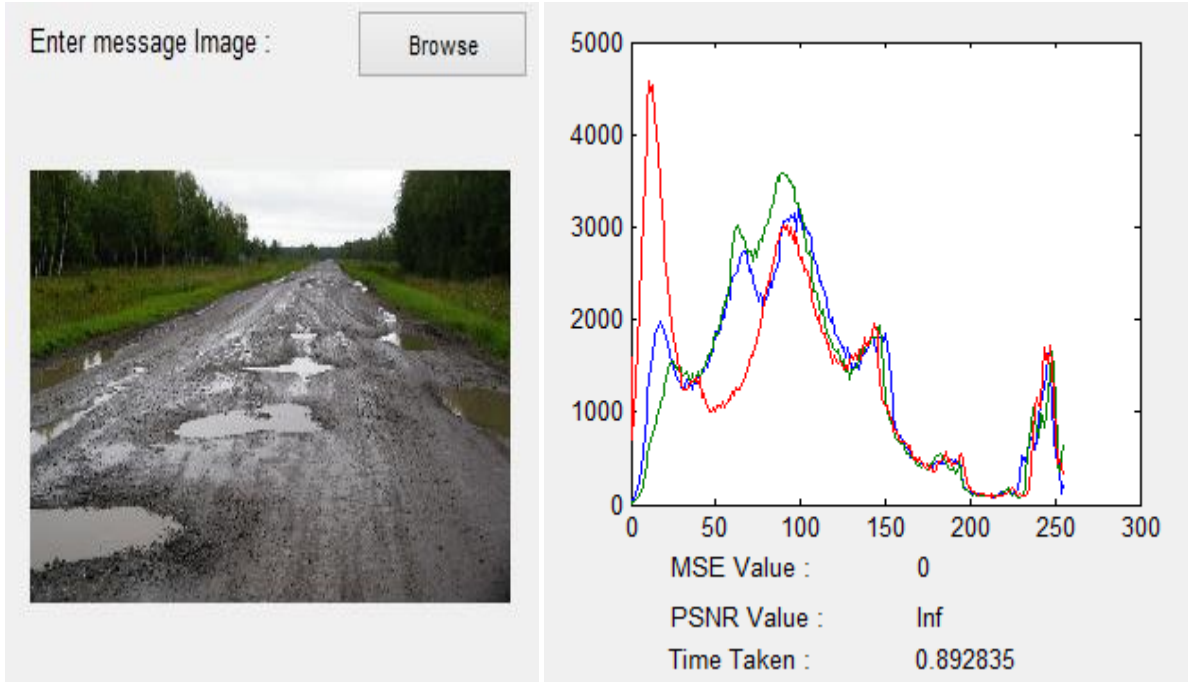


Fig. 4.3 Message image and its histogram sending from sender

Then encrypt that message image using ECC encryption technique after embedding text message data if that text message data is available or entered by sender.

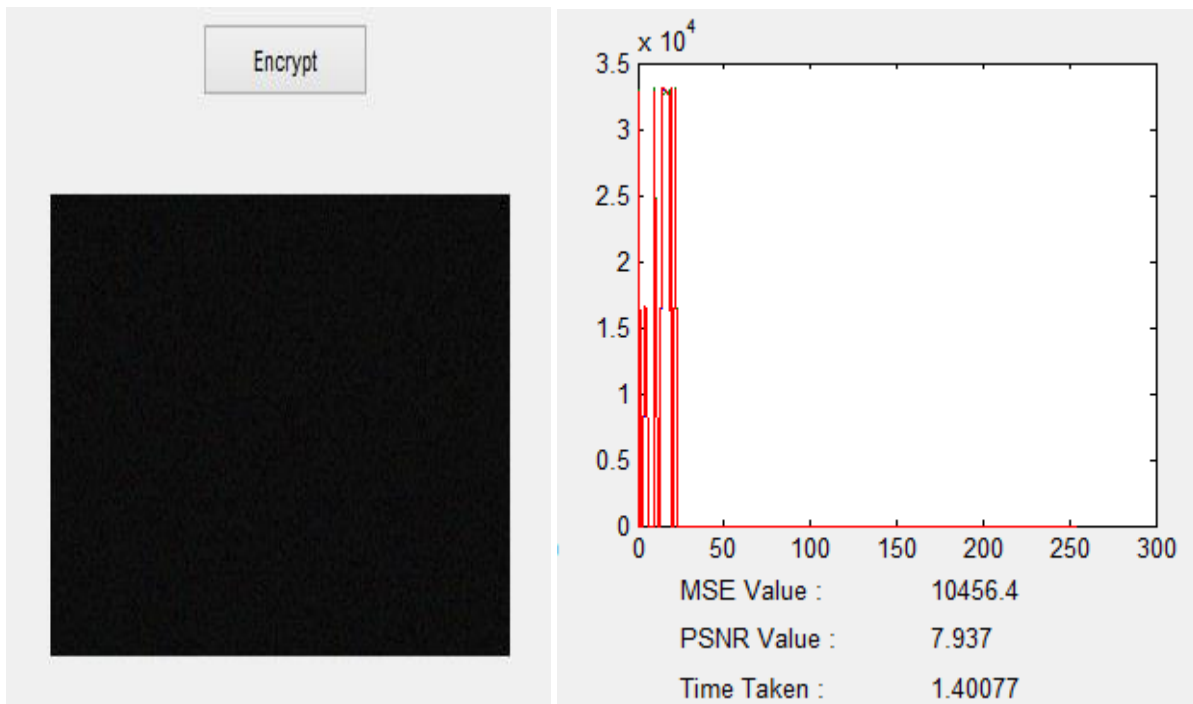


Fig. 4.4 Encrypted Image, its histogram, MSE and PSNR value



Finally that encrypted image is embed with cover image and after that send that image to the particular vehicle.

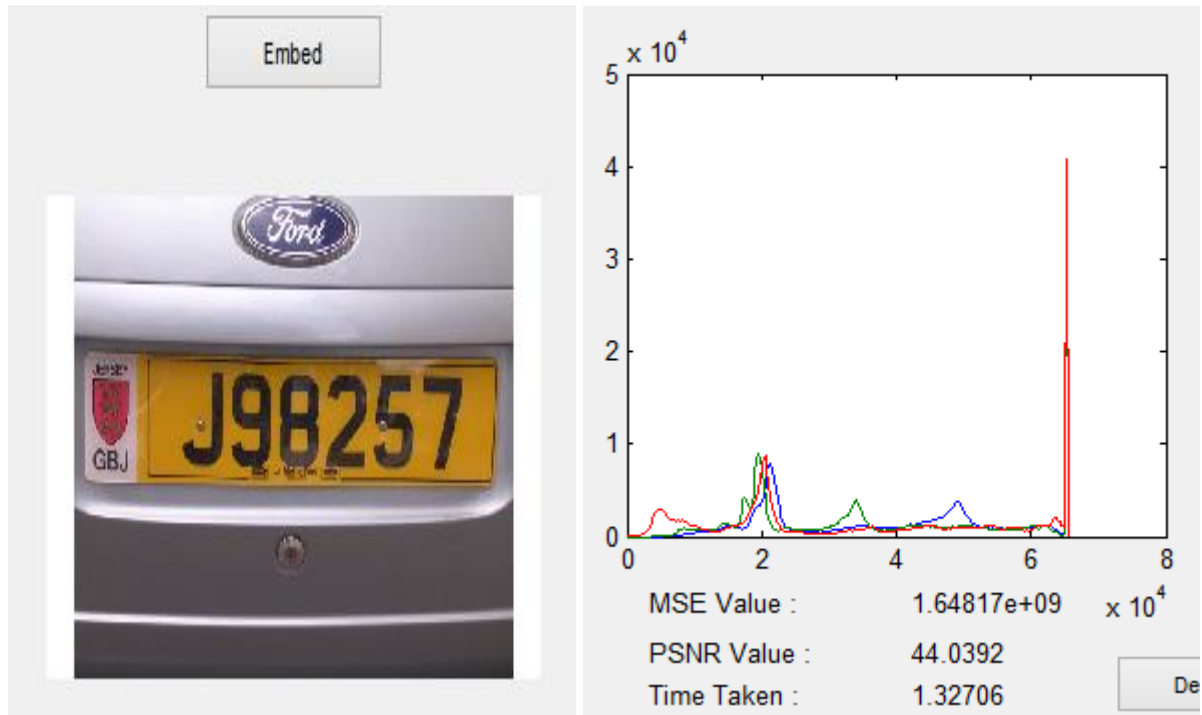


Fig. 4.5 Embedded image, histogram, MSE, PSNR value

### 4.3 Result at Receiver Side

Receiver get that image which is finally generated by sender after encryption and embedding process. Then first of all receiver vehicle's driver separate the encrypted message image and cover image.

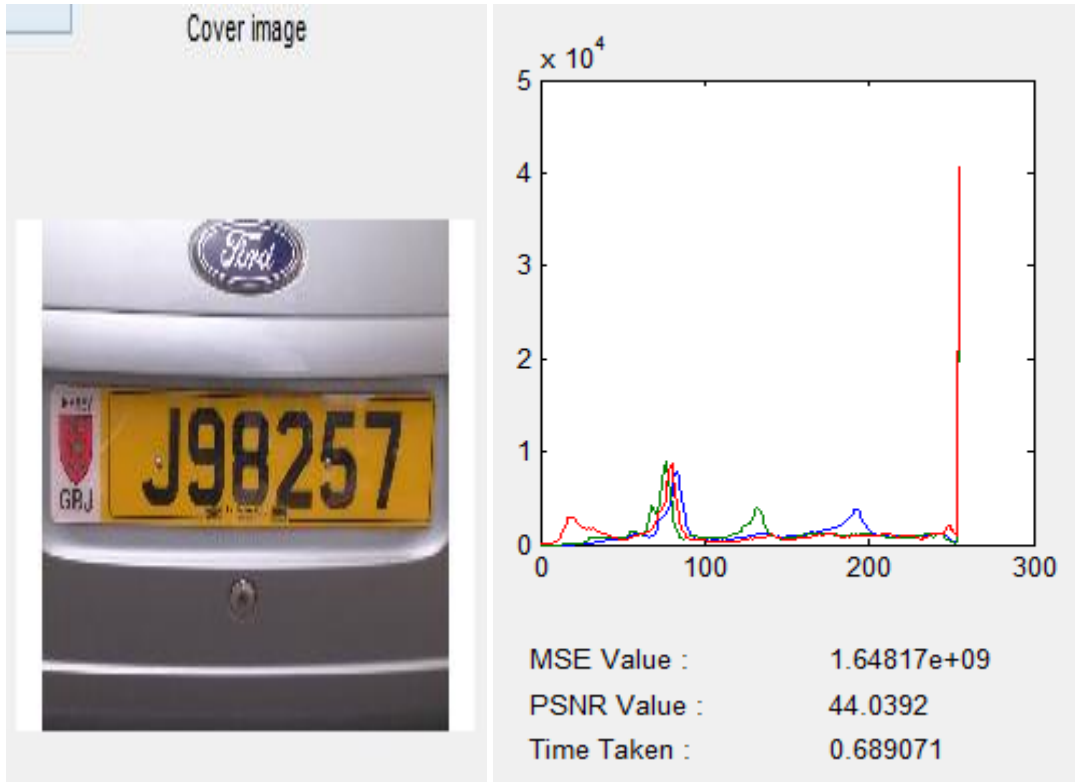


Fig. 4.6 Cover image after separation, its histogram and MSE, PSNR value

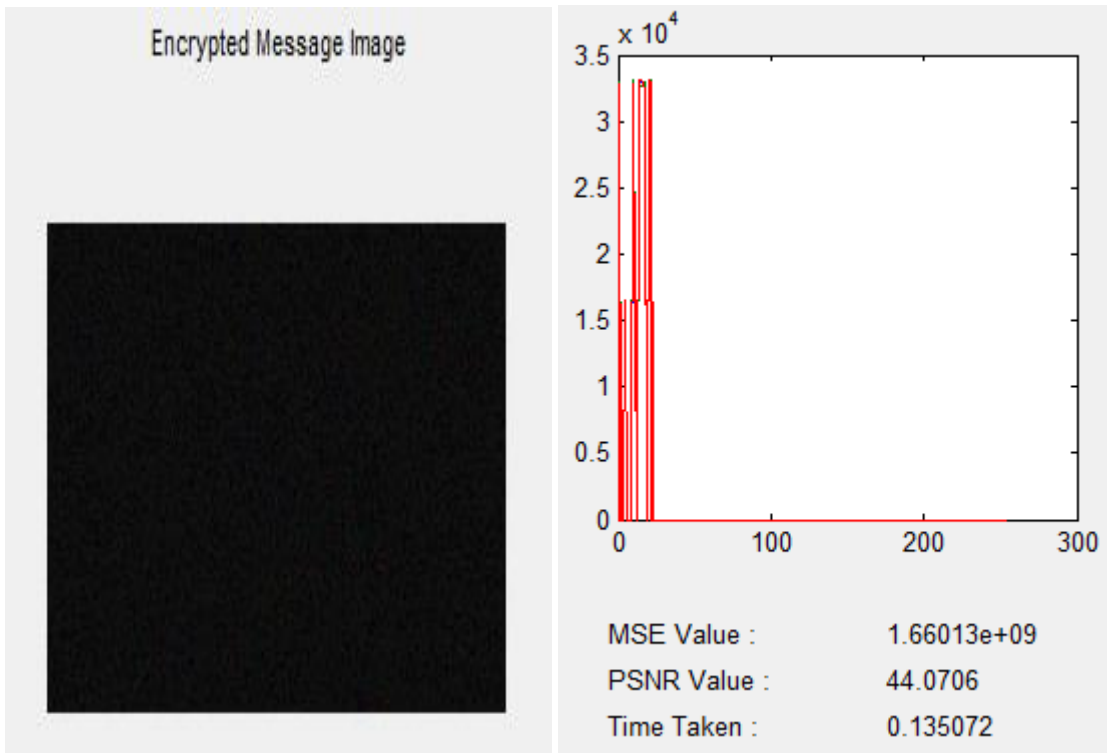


Fig. 4.7 Encrypted Message image after separation, histogram and MSE, PSNR value

Then Receiver decrypt that Encrypted message image using ECC technique and finally get message image and also retrieve the text message data from it.

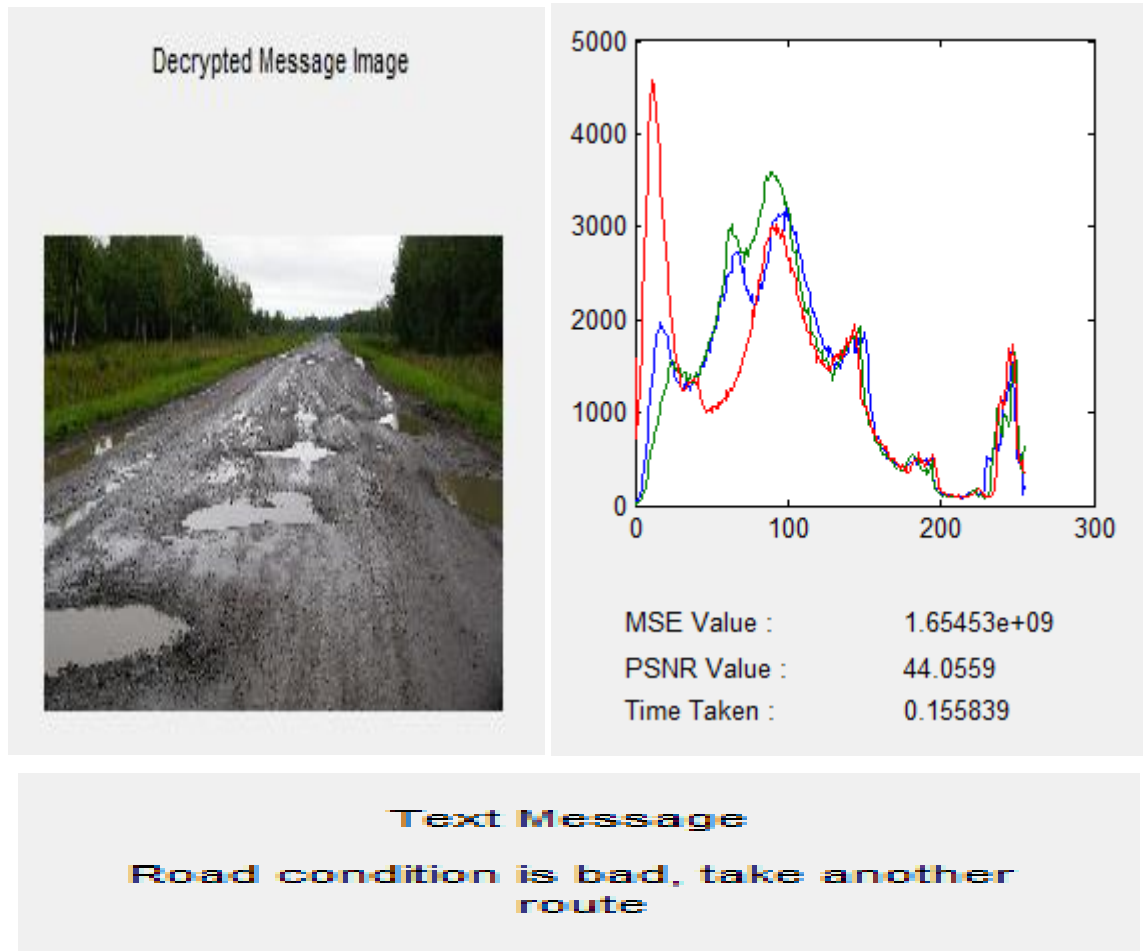


Fig. 4.8 Message Image, histogram, MSE and PSNR value, and Text message data

#### 4.4 Graph representation of MSE, PSNR and Time taken

##### At the Sender Side:

Table 4.1 Values of MSE, PSNR, and TIME taken at Sender side

Sender Side				
	Message Image	Cover Image	Encrypt Image	Embed Image
MSE	0	0	10456.4	1.65E+09
PSNR	Inf	Inf	7.937	44.0392
Time (in Sec)	0.892835	0.621132	1.40077	1.32706

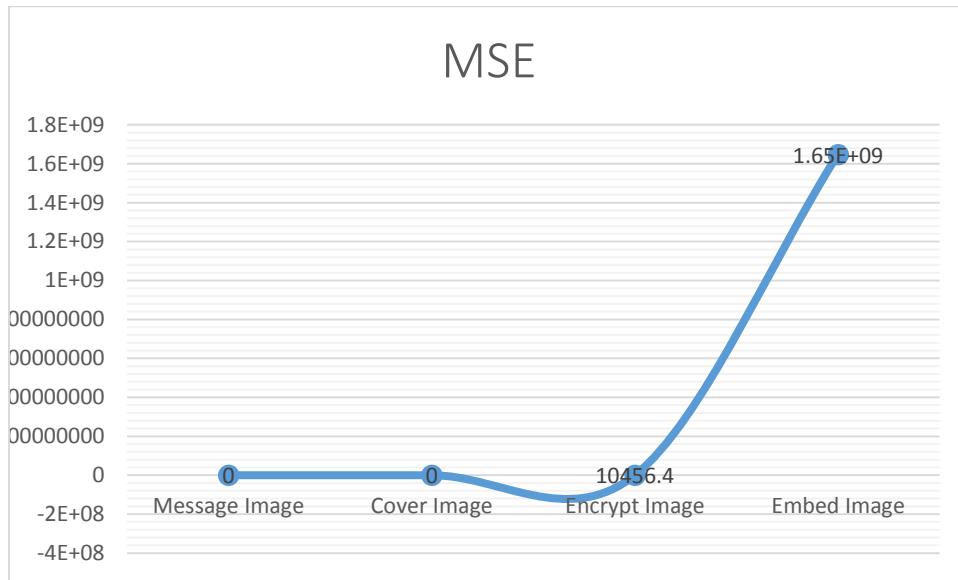


Fig. 4.9 Graph of MSE values at Sender side

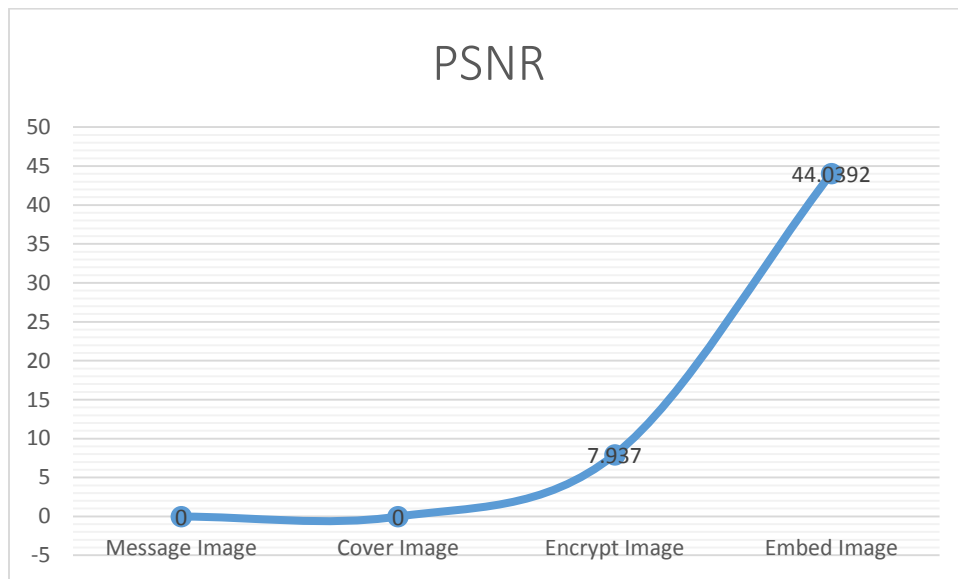


Fig. 4.10 Graph of PSNR values at Sender side

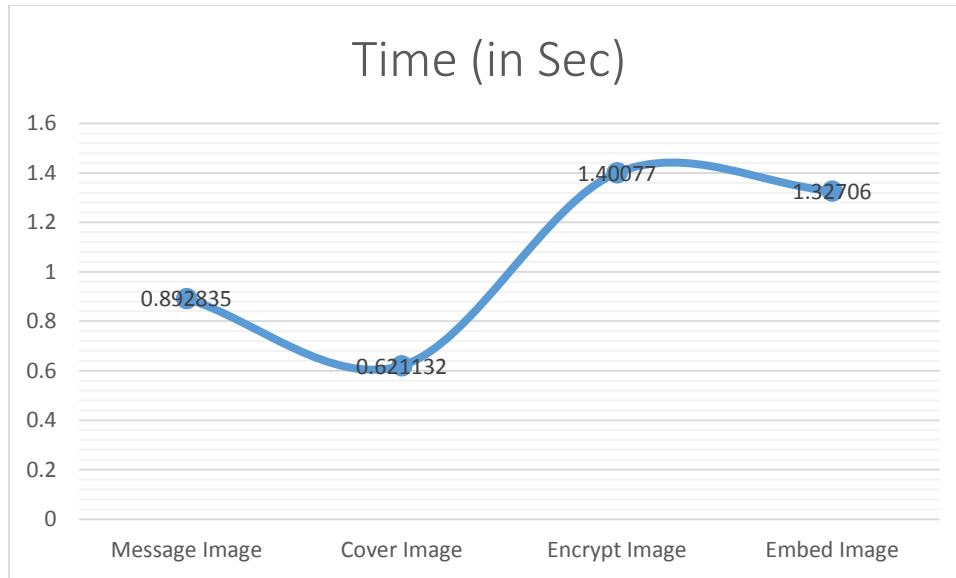


Fig. 4.11 Graph of Time taken at Sender side

**At the Receiver side:**

Table 4.2 Values of MSE, PSNR and Time taken at Receiver side

Receiver Side			
	Cover Image	Encrypt Image	Decrypt Image
MSE	1.65E+09	1.66E+09	1.65E+09
PSNR	44.0392	44.0706	44.0559
Time (in Sec)	0.689071	0.135072	0.155839

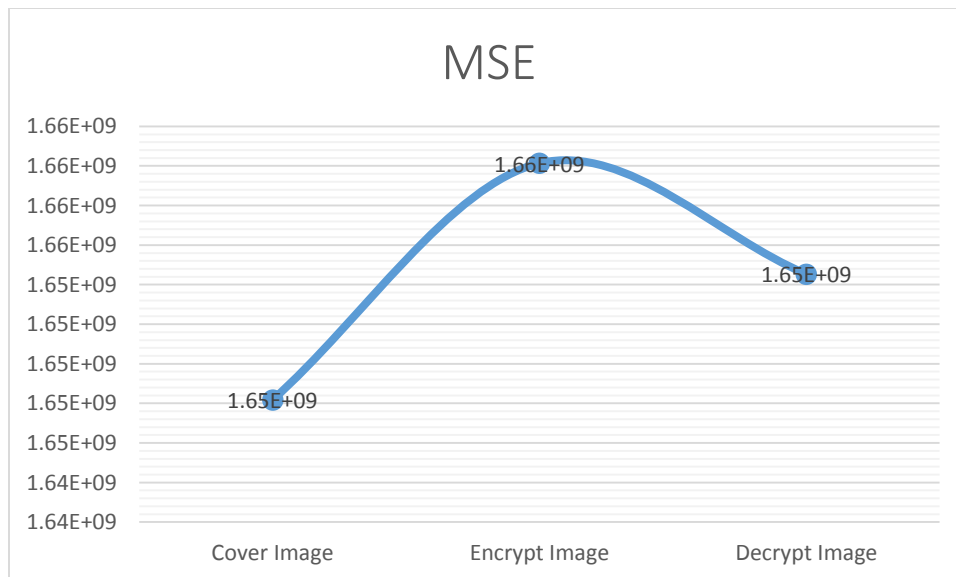


Fig. 4.12 Graph of MSE values at Receiver Side

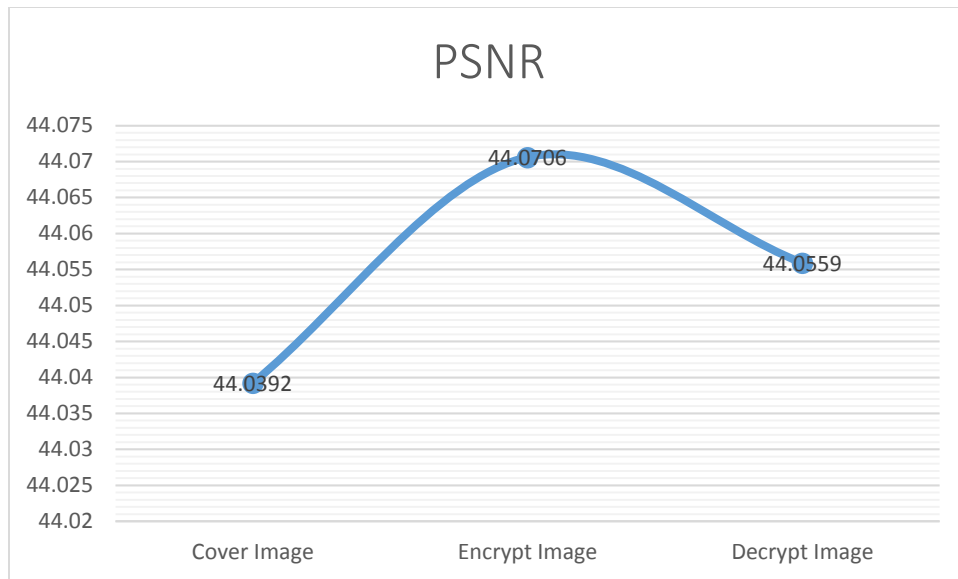


Fig. 4.13 Graph of PSNR values at Receiver Side

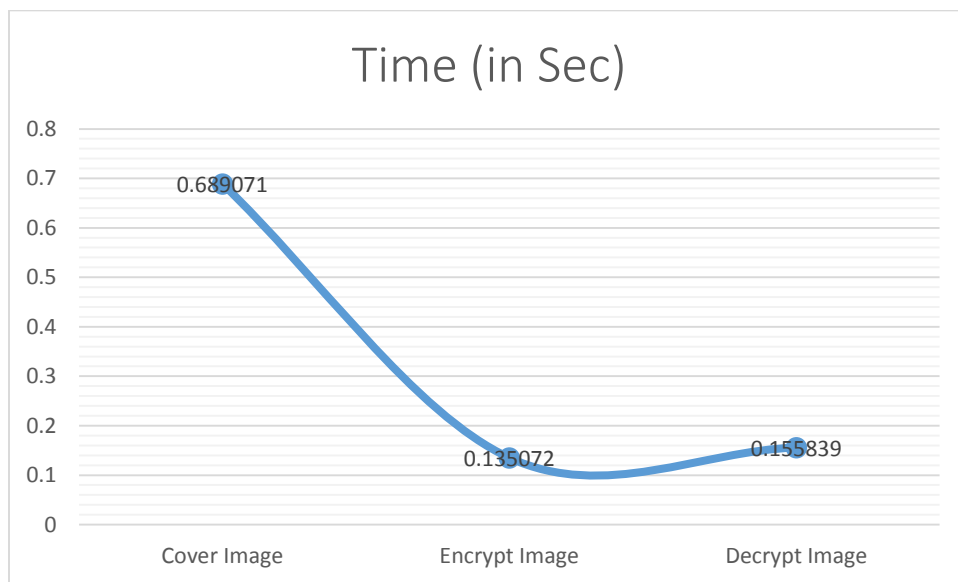


Fig. 4.14 Graph of Time Taken at Receiver side

We also try some different message image with variable size and dimension in our technique, and calculated their MSE, PSNR and Time-taken value at receiver side:

Table 4.3 Comparison of MSE, PSNR and Time value of different dimension's image

Dimension	Message image Size (KB)	MSE Value	PSNR Value	Time Taken
1153 x 1016	137	1.77097	44.3513	1.41365
1545 x 1073	174	1.54417	43.7561	1.62528
1024 x 768	72.6	1.32726	43.0988	1.28178
350 x 240	165	1.57328	43.8373	1.05996

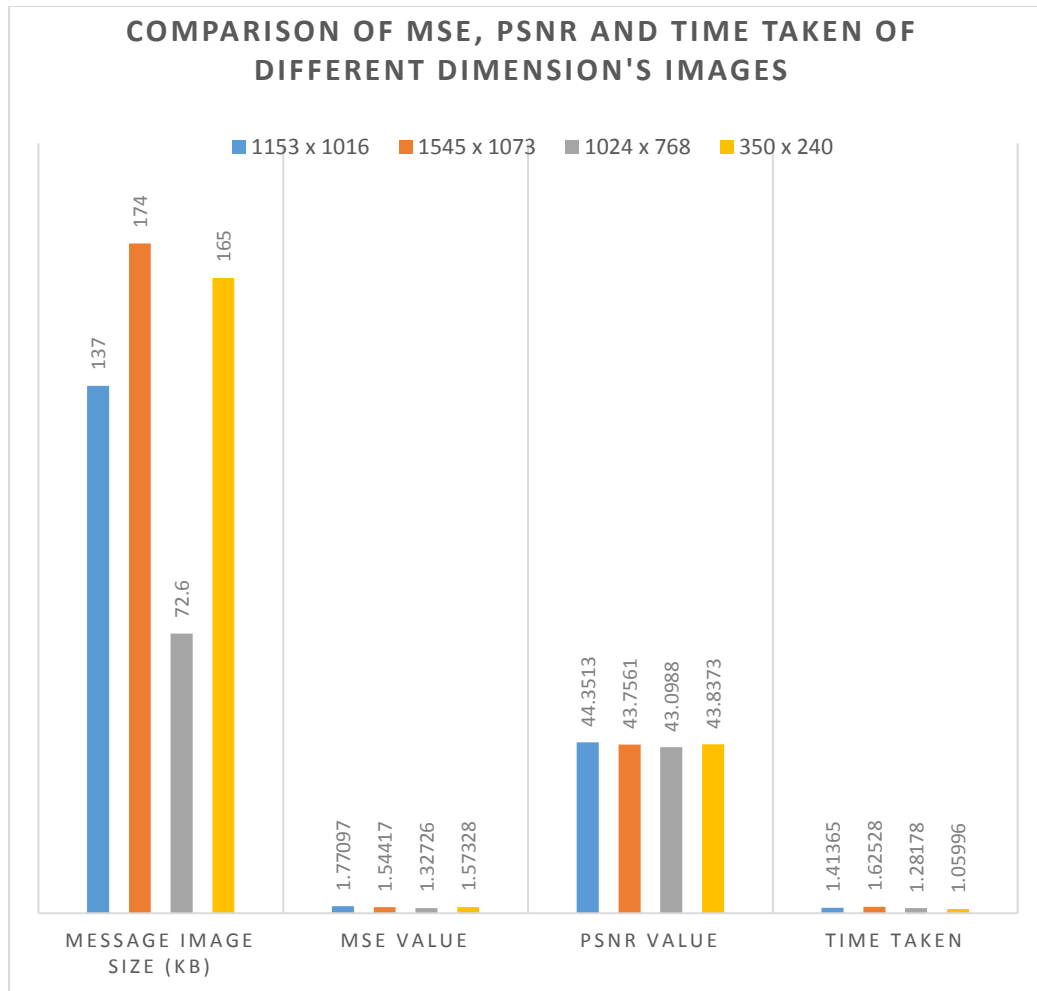


Fig. 4.15 Comparison graph of different dimension's images

We can see that PSNR value is higher than 40db, so it is hard for the human eye to distinguish the distortion in the stego-image.

## 4.5 Comparison between ECC and other asymmetric Encryption Technique

Pretty much as modular exponentiation decided the efficiency of integer factorization and discrete logarithm frameworks, so it is the figuring of  $Q = xP$  for a point  $P$  on the elliptic curve and some number  $x$  which dominates the calculations included in the operation of the ECC. The procedure of including elliptic curve points requires a few modular computations, so in all one of the three cases the operation of a public key cryptographic framework is dependent upon efficient modular arithmetic.

Table 4.4 Comparison between key sizes of ECC and other asymmetric encryption method

<u>Cryptosystem</u>	<u>System parameters (bits)</u>	<u>Public key (bits)</u>	<u>Private key (bits)</u>
<b>RSA</b>	N/A	1088	2048
<b>DSA</b>	2208	1024	160
<b>ECC</b>	482	161	169

Table 4.5 Comparison of Signature sizes on long messages (e.g. 2000-bit)

<u>Cryptosystem</u>	<u>Signature size (bits)</u>
<b>RSA</b>	1024
<b>ELGAMAL (DSA)</b>	320
<b>ECC</b>	320

Table 4.6 Comparison between sizes of encrypted 100-bit messages

<u>Cryptosystem</u>	<u>Encrypted message (bits)</u>
<b>RSA</b>	1024
<b>ELGAMAL (DSA)</b>	2048
<b>ECC</b>	321



Subsequently ECC offers considerable bandwidth saving data transmission over the other types of public key cryptographic frameworks while being utilized to transform short messages. In summary, the ECC gives greater efficiency than either number factorization system, in terms of computational overheads, key sizes, and transmission capacity. In executions, these savings mean higher rates, lower power utilization, and code size reductions.

## 4.6 Timeline

Table 4.7 Timeline Gantt-Chart

Timeline Gantt Chart			
Description	Start month	End Month	Duration (Days)
Review of Literature	Aug-14	Sep-14	60
Problem Formulation	Sep-14	Oct-14	60
Algorithm Formulation	Oct-14	Nov-14	60
Results and Analysis	Jan-15	Feb-15	58
Report Writing	Mar-15	Apr-15	60

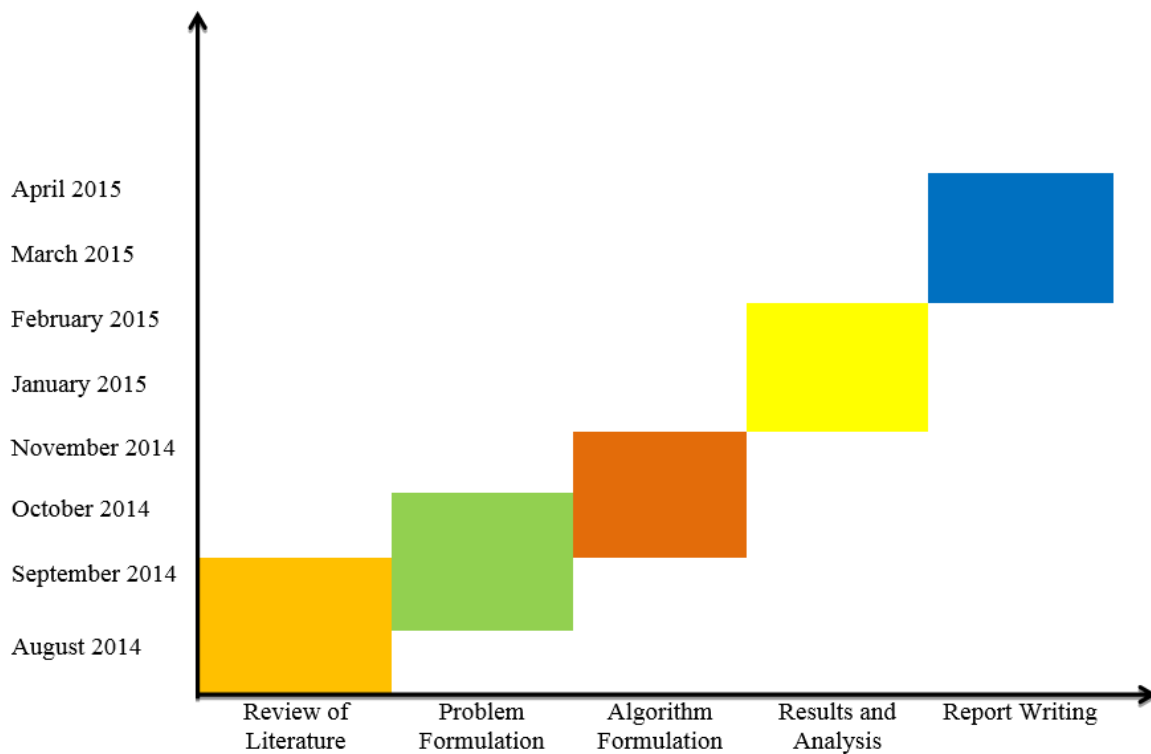


Fig. 4.16: Timeline report graph

## CHAPTER 5

# CONCLUSION AND FUTURE SCOPE

---

VANET is a very sensitive thing regarding security. It is used to harm other person or get benefit from it, directly by alter the data during transmission or by sending wrong message to another or by representing at the receiver that sender is legitimate user but he is not.

So, for stop those attacks on VANET there is ECC and Steganography, both techniques are going to use in the above proposal. Here ECC is used for provide more security and faster encryption and decryption on the message than other techniques. Steganography is used to hide the messages from other intruders, and if message image and cover image having different sizes then also embedding of both are easily. The Purpose of using steganography in it, that third party wouldn't know that there is any hidden message on it only by seeing that message. A novel approach of variable size image and text size image embedding behind the cover image is proposed, which enhances the secrecy of valuable data using B-E&D and E-O Toggle approach. Authentication of vehicle driver is achieved using asymmetric key encryption scheme Elliptic Curve Cryptography. Text message embedding using E-O Toggle approach has one limitation, i.e. the 8 bit- binary representation of text message should be less than or equal to the cover image bits. Otherwise, the text message will be truncated. In future, we will try to remove the above mentioned limitation of E-O Toggle approach. Implementation of the proposed algorithm will be done in MATLAB.

## CHAPTER 6

# REFERENCES

---

- A. E. Mustafa, A. M. (2011). A Proposed Algorithm for Steganography in Digital Image Based on Least Significant Bit. *Research Journal Specific Education*, 752-767.
- Aditya Sinha, P. S. (2014). Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack. *International Journal of Computer Application*, 14-17.
- Asif Ali Wagan, B. M. (2010). VANET Security Framework for Trusted Grouping using TPM hardware. *IEEE*, 309-312.
- Asif Ali Wagan, B. M. (2010). VANET Security Framework for Trusted Grouping using TPM Hardware :Group Formation and Message Dissemination. *IEEE*, 607-611.
- Chetan V.S, N. S. (2013). Security Framework for VANET for Privacy Preservation. *IEEE*, 29-34.
- Chin-Chen Chang, Y.-C. C.-C. (2009). A Steganographic Scheme Based on Wet Paper Codes Suitable for Uniformly Distributed Wet Pixels. *IEEE*, 501-504.
- F. Amounas, E. H. (2012). ECC Encryption and Decryption with a Data Sequence. *Applied Mathematical Science*, 5039-5047.
- Ghassan Samara, W. A.-S. (2012). Security Analysis of Vehicular Ad hoc Networks (VANET). *IEEE*, 55-60.
- Jun Shao, X. L. (2015). A Threshold Anonymous Authentication Protocol for VANETs. *IEEE*, 1-9.
- Manish Kumar Soni, A. V. (2014). Secure Enhance Protocol for Vehicular Ad-hoc Networks. *IJCSIT*, 1020-1022.
- Nurain Izzati Shuhaimi, T. J. (2012). Security in Vehicular Ad-hoc Network with Identity-Based Cryptography Approach: A Survey. *IEEE*, 276-279.
- U. Rizwan, H. F. (2012). A New Approach in Steganography using different Algorithms and Applying Randomization Concept. *International Journal of Advanced Research in Computer and Communication Engineering*, 660-667.
- Vijay Kumar Sharma, V. S. (2012). A Steganography algorithm for hiding image in image by improved LSB substitution by minimize detection. *Journal of Theoretical and Applied information technology*, 1-8.
- Zou, B. A. (2009). Distributed Certificate Architecture for VANET. *Springer*, 26-27.

# CHAPTER 7 APPENDIX

---

## LIST OF ABBREVIATION

<b>OBU</b>	On-Board Unit
<b>RSU</b>	Road Side Units
<b>E-O Toggle</b>	Even Odd Toggle
<b>MSE</b>	Mean Square Error
<b>TTP</b>	Third Trusted Party
<b>LSB</b>	Least Significant Bit
<b>VLP</b>	Vehicle License Plate
<b>TPD</b>	Temper Proof Devices
<b>PKG</b>	Private Key Generator
<b>TA</b>	Central Level Authority
<b>TPM</b>	Trusted Platform Module
<b>VANET</b>	Vehicle Ad Hoc Network
<b>MANET</b>	Mobile Ad Hoc Network
<b>PKI</b>	Public Key Infrastructure
<b>QLA</b>	Queue Limiting Algorithm
<b>PSNR</b>	Peak Signal-to-Noise Ratio
<b>CRL</b>	Certificate Revocation Lists
<b>ECC</b>	Elliptic Curve Cryptography
<b>IBC</b>	Identity Based Cryptography
<b>B-E &amp; D</b>	Bit-Level Extend and Dwindle
<b>CTA</b>	City Level Trusted Authorities
<b>RVC</b>	Road-Vehicle Communications
<b>STA</b>	State Level Trusted Authorities
<b>IVC</b>	Inter-Vehicular Communications

<b>ITS</b>	Intelligent Transportation System
<b>VPKI</b>	Vehicular Public Key Infrastructure
<b>APDA</b>	Attacked Packet Detection Algorithm
<b>DSRC</b>	Dedicated Short Range Communication
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>WAVE</b>	Wireless Access in Vehicular Environments

## GLOSSARY OF TERM

**Anonymity:** Hiding the identity of the vehicle.

**Authentication:** The assurance that the communicating entity is the one that it claims to be.

**Certificate Revocation List (CRL):** A list vehicles with invalid identities.

**Conditional Privacy:** Related to anonymity and tracing.

**Confidentiality:** Protection of message from unauthorized disclosure.

**Decryption:** Changing the cipher text back to the plain message.

**DSRC:** Dedicated short-range communications are on-way or two-way short-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards.

**ECC:** Elliptic Curve Cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

**ECDSA:** Elliptic Curve Digital Signature Algorithm offers a variant of the Digital Signature Algorithm which uses ECC.

**Encryption:** Transforming the plain message to a cipher text.

**On-Board Units (OBU):** Devices mounted on vehicles to facilitate wireless communication.

**Private Key:** A secret key.

**Public key:** A key shared by everyone.

**Road-Side units (RSU):** Communication units located aside the road that connects to the application server and the trusted authority.

**Steganography:** It is a technique to hide a file, message, image, or video within another file, message, or video.

**TPD:** Tamper proof device is resistance to tampering by either the legitimate user or malicious users of system with physical access to it.

**Trusted authority:** A third party who performs certificate generation, issue and revocation.

**TTP:** A Trusted Third Party is an entity which provide interaction between two vehicles who both of them trust on the Third Party.

**UID:** Acronym for unique identification number, it is a unique number assigned to each vehicle that registers itself with the RSU.

**VANET:** A technology that allows vehicles to form a network and communicate with one another, as well as the roadside infrastructure.

## MEANING OF NOTATION

<b>Notation</b>	<b>Meaning</b>
BI	Background Image
CI	Cover Image
$S_i$	Result Image
$X_1, X_2, X_3$	Matrixes
$TU_j^i$	Input Text Messages
RI	Received Image
RBI	Received Background Image
RCI	Received Cover Image