Application Of ECC And ECDSA For Image With Error Control Technique Using RS Code

G Shruthi Sastry, Dr. Smitha Sasi

***Abstract*— The best approach to verify conveyed multimedia applications is to scramble multimedia data utilizing public key cryptography calculations. Elliptic curve method of cryptography is a strategy that implies ensuring private data against unapproved access in that circumstance where it is hard to give physical security. The paper proposes an answer for keep up authentication of the ECC encrypted image transmission by including ECDSA that is utilized to deal with the confirmation of key exchange with the trusted entities. Reed-Solomon(RS) codes are utilized to perform Error Correction for the errors that occur upon the data. RS codes are usually utilized in the digital communication because of their solid abilities to wipe out both random as well as burst errors. FEC encoders present redundancy in data before it is transmitted. The repetitive data are transmitted alongside the original data through the channel. A RS decoder at the end is utilized to recuperate any undermined data.**

***Index Terms*— ECC, ECDSA, encrypt, erasures, error location, decrypt, keys, polynomial, Reed soloman, syndrome.**

I. INTRODUCTION

The errors are the typical event in digital communication systems, broadcasting systems and digital storage gadgets. Numerous systems have conceived to alleviate this issue. Forward error correction is a procedure in which redundant data is added to the message, with the goal that a few errors can be remedied at the recipient, utilizing the additional redundant data.

Reed Solomon is an error-correcting coding system that was contrived to address the issue of correcting various errors particularly burst-type errors in mass storage gadgets like HDD, DVD, wireless and mobile communications units, satellite connections, digital TV, DVB and modem (xDSL).

Reed-Solomon codes are a significant subset of non-binary cyclic error correcting code and are the most generally utilized codes practically speaking[14,15]. These codes are utilized in wide scope of uses in digital communications and data storage.

which at last outcomes in errors in the got data. Along these lines, error control is utilized to help streamline the exactness and unwavering quality of the transmission. Error control is a strategy that can recognize and address errors. For the most part, there are two ways of error control: the first is that, once errors are found, the decoder naturally corrects these errors dependent on specific standards; another strategy is that once errors happen, rather than correcting the errors, the less than desirable end sends a feedback signal to the transmitting end revealing to it that errors happened and demands that message to be sent once more to the transmitter.

G Shruthi Sastry, Student, MTech, Digital Communication and Networking, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

Dr. Smitha Sasi, Associate Professor, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

II. LITERATURE SURVEY

The equation of the elliptic curve on a binary field is $y2 + xy = x3 + ax2 + b$, where $b \neq 0$[1]. Here the components of the finite field are numbers of length at most m bits. These numbers can be considered as a binary polynomial of degree m – 1. In binary polynomial the coefficients must be 0 or 1. The entire task, for example, expansion, subtraction, division, multiplication includes polynomials of degree m – 1 or lesser. The m is picked with the end goal that there is finitely huge number of points on the elliptic curve in order to secure the strength of cryptosystem. The numeric and alphabetic character in the plaintext is expressed by its ASCII value [8]. Considering points on the elliptic curve, the ASCII value is mapped to the point on the curve for encryption.

The utilization of affine points for the purpose of plain text transformation to its ASCII value it is benefit of this approach[2]. This transformation's purpose is two folds. First, a single digit of the character's ASCII integer is converted into a set of coordinates to confine within the Elliptic curve. Secondly, the non-linearity is brought out by the transformation in the character covering its identity. The ECC technique is incorporated to encrypt the data in the form of a transformed cipher text. Without the knowledge of private key, the decryption of the original information is infeasible. [3]. RSA is considered as the first real life and practical asymmetric-key cryptosystem. It becomes de facto standard for public-key cryptography. Its security lies with integer factorization problem. RSA's decryption process is not efficient as its encryption process. The comparison of RSA and ECC is made by performing encryption and decryption on three example input information of 8 bits, 64 bits, 256 bits with random keys dependent on NIST suggestion. In light of experimentation, it was discovered that ECC beats RSA in regards to operational proficiency and security with lesser parameters. An ECC is especially most appropriate for devices with limited resources. Compared to RSA, the pith of ECC is that it appears to provide better security for a smaller key size, thus reducing overhead processing [13]. The ability of RSA is insufficient due the prerequisite of expansive number of bits. RSA calculation can be moderate in situations where extensive data should be encoded by a similar PC. It requires a third party to confirm the dependability of public keys. Data exchanged through RSA calculation could be undermined through go betweens who may temper with the public key framework [5, 6].

III. REED SOLOMON CODES

The ReedSolomon codes are dependent on the finite fields. In the event that the quantity of elements on a field F is finite, this field is known as a finite field, or a Galois field. The quantity of elements is known as the order of the field. Galois field F = {0 1, 2, … , - 1} is a finite field with modulus p and order p and it tends to be spoken to as GF (p). Number p is a prime number. A polynomial over a field is a polynomial of which the coefficients are the elements of a Galois field GF(p). The polynomial over GF(p) is given by,

$$P(x)= a_0+a_1(x)+a_2(x^2)+.....+ a_p(x^p)$$

where, $a_i \epsilon F, i = 0, 1, 2,\ldots,p.$

A Reed Solomon code is a block code, implying that the message to be transmitted is isolated up into independent blocks of data. Each block at that point has parity insurance data added to it to shape an independent code word. It is additionally a systematic code, which implies that the encoding procedure does not change the message and the security bits are included as a different piece of the block. Likewise, a Reed Solomon code is a linear code(adding two code words creates another code word) and is cyclic(cyclically moving the symbols of a code word delivers another code word). It resembles with the group of BCH codes, however is recognized by having multi-bit symbols. In this way a Reed Solomon code can be portrayed as a (n, k) code, where n is the block length and k is the quantity of information bits.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

It is one of the public key cryptographic techniques which have vital application in securing of data in the form of encryption. In public key cryptography every client participating in the data transaction has a couple of keys, namely, a public key ECC is an abbreviation for and a private key. The cryptographic computations are performed by these keys [6]. The private key is known to the specific user while the public key is communicated to all the users in the network. The public key algorithm needs a lot of predefined constants to be known by all the devices participating in the communication such as domain parameters p, a, b, G, n and h. p is the prime number characterized for finite field Fp. a and b are the parameters characterizing the curve[2]. G is the generator point (xG, yG), a point on the elliptic curve picked for cryptographic operations as shown in fig 1. n is the order of the elliptic curve and h is the cofactor. Each estimation of the 'a' and 'b' gives an alternate elliptic curve. The numerical operations of ECC is characterized over the elliptic curve,

$$y^2 = x^3 + ax + b$$

Where,

$$4a^3 + 27b^2 \neq 0.$$

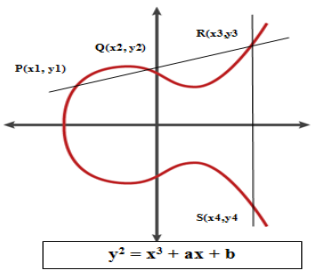

Fig 1 : EC curve and general equation

V. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

ECDSA Python module is capable of handling and getting implemented into several protocols and has the proficiency of generating the keys and signatures of relatively shorter lengths in contrast to other techniques taking minimal time. There is a rich set of resource of random numbers for formation of keys. The signing key and the verifying key have correspondence with the particular standard elliptic curves defined in the library. The security offered by the curves is high for longer lengths of the keys and signatures. ECDSA comprises of two stages, namely, signature generation and signature verification. The signature and the message are sent to the receiver. As the receiver has public key of the sender and its own private key, it is capable of verifying the signature and thus proves whether the information is received from the trusted user or not [7, 8, 9].

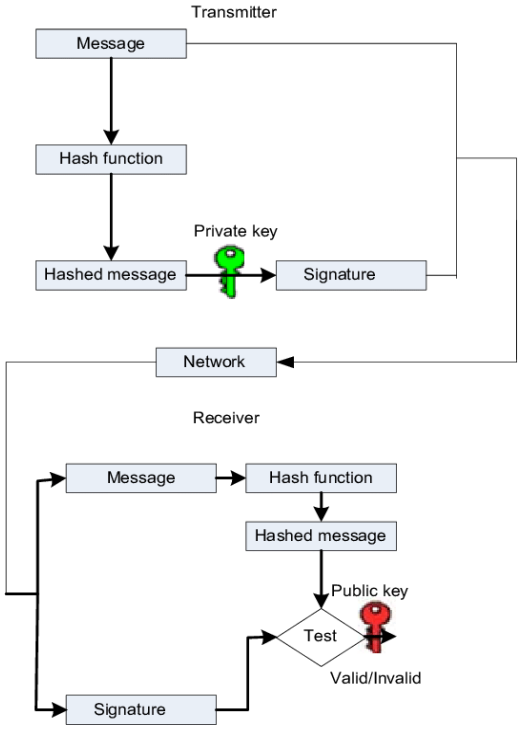

Fig 2 : Ideal model view of ECDSA

VI. METHODOLOGY

The entire cryptographic system is implemented in Python 2.7. The image is read as binary and converted into pixels. A NIST standard prime elliptic curve P-384 is considered for encryption. The domain parameters of the curve specifically, the constants 'a' and 'b' modelling the elliptic curve are of length 384 bits [12]. The prime number 'P' and the order of the curve 'n' are also of length 384 bits long. The total number of points present on the considered P-384 curve is the order ' n' of the curve. The domain parameters 'a', 'b' and 'P' consists of 96 hexadecimal digits summing to 384 bits (96 * 4 = 384). The value of cofactor of P-384 prime curve is one. The various curve points are mapped to the pels of the image. With the help of Python modules 'pyecc', 'ECDSA' and 'hashlib', the encryption and decryption are performed for image data.

Also, digital signature is applied for the encrypted data for authentication. The key pairs are created for signing. SHA-1 algorithm is applied to the encrypted content of data. This process converts the string of arbitrary length into a digest that is of fixed length. This resulting content is converted into integer or hex value. The resultant value of the digest generated consists of 40 hexadecimal digits summing upto 160 bits (40 * 4 = 160). The signature is generated for this value of the digest with the help of methods defined in the class of 'ECDSA' python library. For the purpose of verification of this signature generated, first load the verifying key and signature. SHA-1 algorithm is again applied on the received encrypted data Pc and the digest obtained is converted into integer or hex value. By using the 'verify' method defined in the class of 'ECDSA' module, the signature is compared against the digest computed as shown in fig 2.

On attaining match of this value, the authentication is said to be accomplished. Further, the error controlling mechanism is applied to the encrypted data for the prevention of erroneous data transmission to the receiver that creates ambiguity to the information being decoded at the receiver. Reed Solomon technique is used that introduces three errors in the codeword. These altered data bit positions are detected and corrected. Thus the data travelling through the medium or channel is made to be error free.

A. Procedure for encryption and decryption of an image

1. Consider an image as input X with dimension M×N .
2. The picture elements of the input image are referred to as 'message' that is denoted by the letter 'm'.
3. 'm' is transformed into a point on the curve (Xi,Yi), which is denoted as Pm = (Xi, Yi).
4. All the pixels are similarly mapped to the (x,y) coordinate pairs that are generated by the procedures of operations on the elliptic curve. By substituting the x value in the elliptic curve equation, the corresponding value of 'y' can be obtained from the general equation, $y2 = \{(x3 + ax + b) (\text{modulo } P)\}$ where, P is the large prime integer.
5. The sender chooses a private key Ka; a large integer the receiver chooses a private key Kb; a large integer.
6. A generator point G = (Gx, Gy) is noted from the curve.
7. The sender derives a public key Pa by multiplying its private key with the generator point, Pa = Ka * (Gx , Gy).
8. The receiver derives a public key Kb by computing the product of its private key with the generator point, Pb = Kb * (Gx, Gy).
9. The public keys of both the users are shared among them. While Pm forms the mapped data of the original message to be encrypted, the cipher data Pc is formulated as follows, Pc =(Pa , Pm+ Ka Pb) =Pc (X , Y) . This is the encrypted data that the sender transmits to the receiver. At the receiver, the original information can be retrieved by applying receiver's private key Kb. Multiply the first point with receiver's private key Kb and add it to second point. Pm = (Pm+ Ka PB - Kb Pa) = Pm (Xi ,Yi)

B. Algorithm for ECDSA Signature Generation

1. pick a random number k in the interval, $1 \le k \le \{p - 1\}$
2. Find the point k* (Gx, Gy) = (X1,Y1)
3. Find r = X1(mod P).
4. if r=0 then
   Go back to step 1.
   End if
5. Find, $k-1(\text{mod } P)$.
6. Apply SHA-1 on cipher text Pc and get the integer equivalent of it say e. .
7. Calculate $s = k-1(e + Ka * r)$.
8. if s = 0 then
   Go back to step 1
   end if
9. For encrypted data Pc, the signature is given by, S = (r,s).

C. Algorithm for ECDSA Signature Verification

1. Check if r and s belong to the set of integers ranging in the interval (1,P-1).
2. Find SHA-1 of the encrypted data Pc and the resulting value is converted to integer e.
3. Find the value, $w = s-1(\text{mod } P)$
4. Find out, u1 = e*w(mod P) and u2 = r*w(mod P).
5. Calculate, X = u1Pb + u2Pa
6. if X = 0
   then
   Disagree S
   else
   Calculate the value, V = x1(mod P)
   end if
7. Agree only when V == r.

D. Flowchart

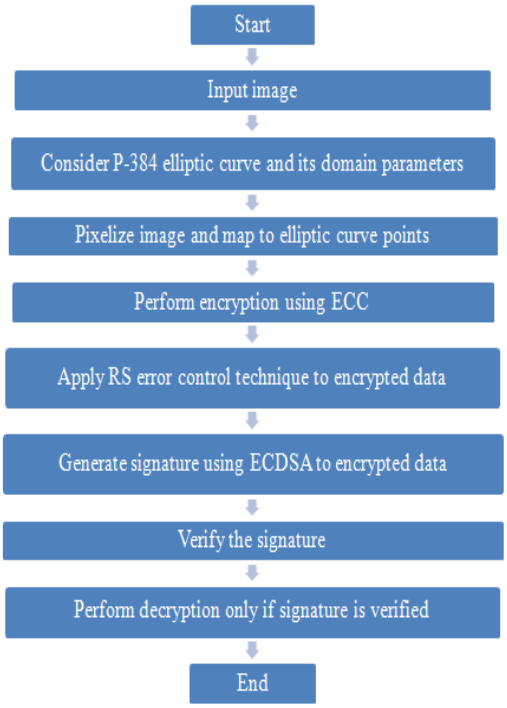

Fig 3 : Flowchart

E. The RS encoder

Reed Solomon Coding is one of the block coding procedure taking single block with k symbols at time and concatenate 2t parity symbols as shown in the figure 4 below.

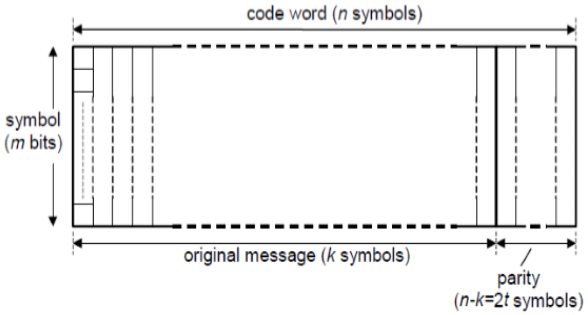

Fig 4 : RS encoder

The g(x) polynomial is defined by :

$$g(x) = \prod_{i=0}^{2t-1}(x + \alpha^i)$$

The encoder sees the block k symbol as a polynomial m(x), whose degree is k-1 and ,MSB's coefficient is the first symbol[14].

Encoder computes the product of M(x) and x2t and div ides it by polynomial g(x) in order to obtain a maximum o f 2t-1 degree polynomial remainder. To construct a polynomial that is fully divisible by g(x), this polynomial should be added to m(x)X2t. An information polynomial m(x) is described by the below expression.

$$m(x) = m_k x^{k-1} + m_{k-1} x^{k-2} + ...m_x x + m_1$$

The code word polynomial c(x) of the RS code is

$$c(x) = c_n x^{n-1} + c_{n-1} x^{n-2} + ...c_2 x + c_1$$

The encoding steps are :

1. Multiply the information polynomial m(x) by Xn-k.
2. Divide m(x) by g(x) to obtain the remainder r(x), i.e. r(x)= m(x)xn-k mod g(x).
3. Derive code word polynomial c(x) through m(x) and r(x), i.e. c(x) = m(x) Xn-k +r(x).

The code word of a RS code is generated with the assistance of the above steps as,

$$C = (C_n, C_{n-1}, ...C_1)$$
$$= (m_k, m_{k-1}, ...m_1, r_{n-k} .....r_1)$$

The starting k symbols denote information symbols , the last r = n-k are parity check symbols. This is the time domain algorithm of RS code and is called as systematic code.

F. Reed Solomon Decoding

The attained code word c(x) by encoding undergoes interference while its transmission across channel. Let noise be e(x) , an error pattern. It is added with c(x) and the resulting sum is transmitted to receiver. Let the polynomial of the vector that is received be r(x), then r(x) = c(x) + e(x). The expressions of c(x), e(x), and r(x) are as follows,

$$c(x) = c_0 + c_1 x + c_2 x^2 + ...c_{n-1} x^{n-1}$$
$$e(x) = e_0 + e_1 x + e_2 x^2 + ...e_{n-1} x^{n-1}$$
$$r(x) = r_0 + r_1 x + r_2 x^2 + ...r_{n-1} x^{n-1}$$

G. Syndromes

The received symbol inputs are divided by the generator polynomial. The result obtaining needs to be zero. The parity bits are appended in the codeword to guarantee the divisibility by the generator polynomial. The remainder left shows the presence of errors. Then remainder is said to be syndrome. The syndromes are calculated by substituting the 2t roots of g(x) in R(x)[15]. The syndrome polynomial's general equation is ,

$$s(x) = s_1 + s_2 x + s_3 x^2 + ...+ s_{2t} x^{2t-1}$$

α is the primary element. si = 0 represents the transmission error; if s≠0, then s appears in transmission, error pattern is determined for error correction.

H. Error-Locator Polynomial

The computation of syndrome polynomial is followed by the error value calculation and corresponding locations. In this step, 2t syndrome polynomials are solved. These polynomials posess _v" unknowns, in which v stands for number of unknown errors before decoding. If these unknown locations are (i1,i2,……iv,) the error polynomial can be given as,

$$E(x) = Y_1 x^{i1} + Y_2 x^{i2} + ...Y_v x^{iv}$$

Yl is the magnitude of the lth error at location il. If Xl is the field element associated with the error location il, then the syndrome coefficients are derived as,

$$S_1(x) = Y_1 X_1 + Y_2 X_2 + ...+ Y_v X_v$$
$$S_2(x) = Y_1 X_1^2 + Y_2 X_2^2 + ...+ Y_v X_v^2$$
$$.$$
$$.$$
$$S_{2t}(x) = Y_1 X_1^{2t} + Y_2 X_2^{2t} + ...+ Y_v X_v^{2t}$$

The above equations set must possess atleast one solution as per the way of definition of the syndromes. This gives unique solution. Thus the decoder's work is to quest the unknowns of the syndromes. This is similar to the problem of solving a system of non-linear equations. The direct solution of the system of nonlinear equations is too difficult for large values of v. Instead, intermediate variables can be computed using the syndrome coefficients Sj from which the error locations, X1, X2 ,....., Xv , can be determined. The error-locator polynomial is introduced as ,

$$\sigma(x) = \sigma_v x^v + \sigma_{v-1} x^{v-1} + ... + \sigma_1 x + 1$$

The polynomial is defined with roots at the error locations −1 i.e Xl-1 for l=1,2,…v. The error location

numbers l, X indicate errors at locations il for l=1, 2, …v
This can be written as,

$$\sigma(x) = (1 - xX_1)(1 - xX_2)\ldots(1 - xX_v)$$

Where, Xl =αil

VII. RESULTS

The image encryption and decryption codes are successfully executed in Python 2.7 operating in Ubuntu platform with the utilization of Python libraries that are featured up with the functionalities supporting the mathematical and logical computations essential for carrying out cryptographic procedures. The encoded data for the image is shown in hex format in the textbox as shown in the figure 6 .The encrypted data is tied up with the RS mechanism to fight against any errors that may occur in the communication process in the channel. The figure 8 shows the generated codeword, error locations and the corrected errors in the codeword. Further, the signing and verification of the sign is also efficiently achieved upon the encrypted data for ensuring the data integrity and authentication as shown in the figures 7 and 9 . The decrypted image is shown in fig 9.

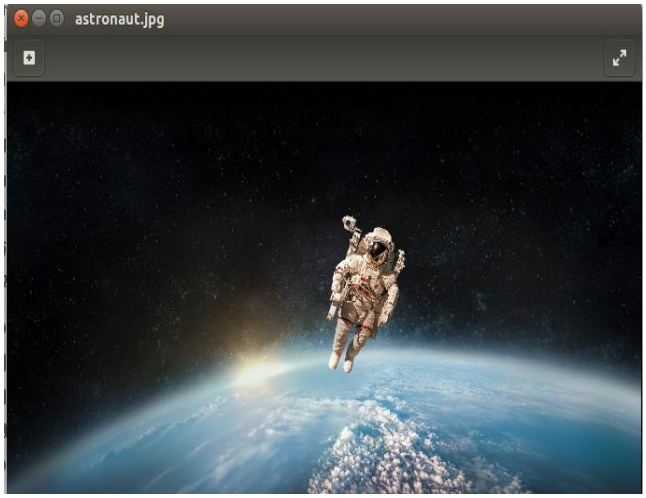

Fig 5: Input image

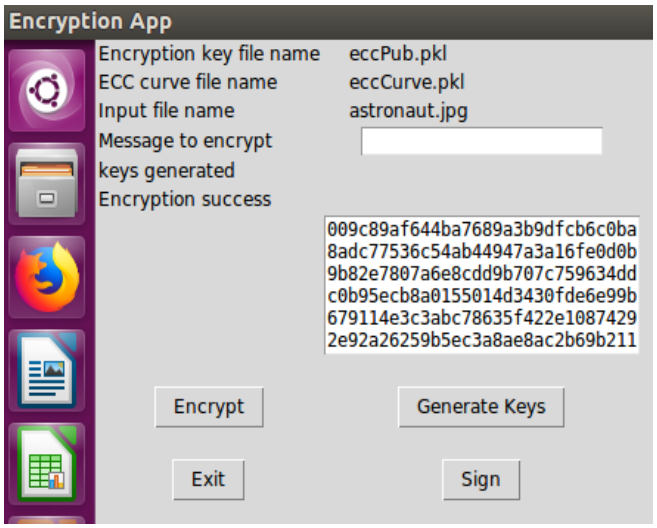

Fig 6 : Encrypted image

Fig7 : Signature generated by the sender

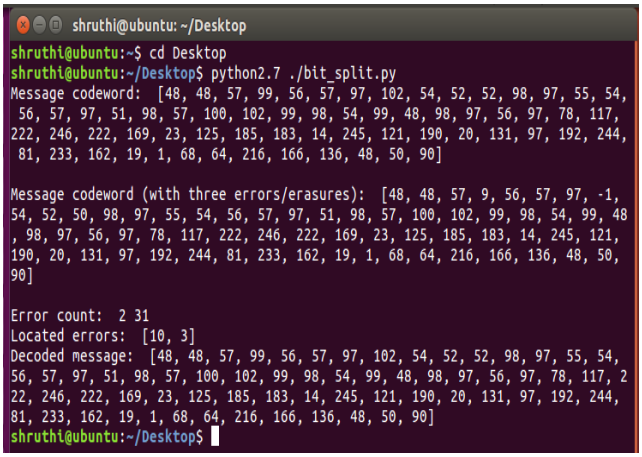

Fig 8 : Error detection and correction

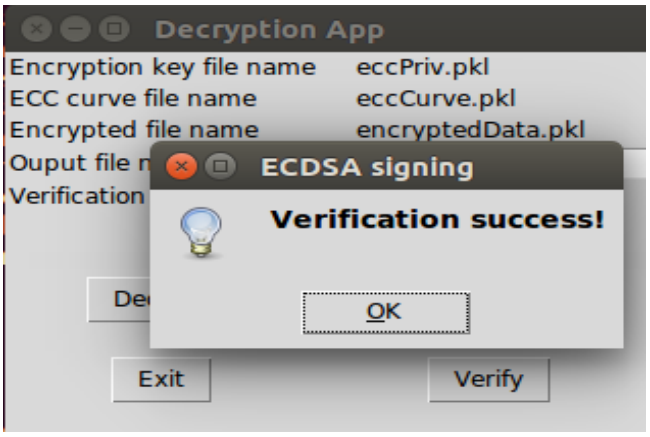

Fig 9 : Matched signature

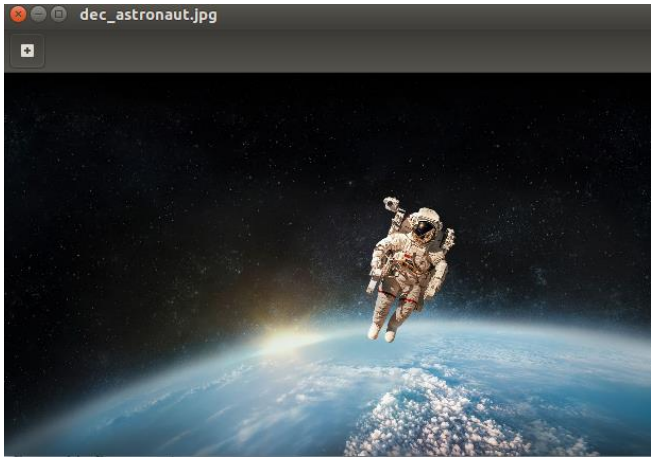

Fig 10: Decrypted image

VIII. CONCLUSION

The cryptographic Elliptic Curve method provides digital signatures including encryption. This component gives authentication to high level of security and secrecy , which guarantees that the data is sent from the particular confided in source. An image considered is scrambled with the ECC system over a prime curve p-384. Hash is applied for the encoded data to resize it to fixed length. A digest of length 160 is gotten and the signature is produced for this digest. The three errors are inserted in the codeword by altering the information. The detection and correction of these errors are accomplished through the aid of RS codes. The verification of the signature is completed at the unscrambling end and the original image is recovered just if the signature is checked. Therefore, the proposed system checks the validness of the source alongside performing encryption and decryption forms and makes the data free from errors.

REFERENCES

[1]Kamlesh Gupta and Sanjay Silakari , " An ethical way for image encryption using ECC" , First International Conference on Computational Intelligence, Communication Systems and Networks, 2017.

[2]Maria Celestin Vigila, K. Muneeswaran, "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography ", IEEE 2015.

[3]Balamurugan.R and Kamalakannan.V, "Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography ", IEEE 2018.

[4]Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security",IEEE Wireless Communications, pp. 62-67,Feb.2016.

[5]Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, " Image Encryption using Elliptic Curve Cryptography" , Eleventh International Multi-Conference on Information Processing", 2015 (IMCIP-2015)

[6]Nissa Mehibel and Mohammed Hamadouche, " A new algorithm for a public key cryptosystem using elliptic curve", 2017 IEEE European Conference on Electrical Engineering and Computer Science.

[7]Ravi Kishore Kodali ," Implementation of ECDSA in WSN", International Conference on Control Communication and Computing (ICCC), 2016

[8]Li Hui-na and Ping Yuan, " A simple limited one time authorization mechanism based on ECDSA" , ICACT 2012.

[9]Yoppy Sazaki Megah Mulya, " The development of android based SMS security using ECDSA with Boolean permutation", IEEE 2016 .

[10] Zhang Chuanrong, Chi Long ," Secure and efficient generalized signcryption scheme based on short ECDSA", IIHMSP 2018.

[11] Karthik Kedarisetti and Roopesh Gamini, " Elliptic curve cryptography for images using fractal based multiple key hill cipher", ICECA 2018.

[12] Certicom, "Standards for Efficient Cryptography", SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2016.

[13] Dindayal Mahto and Dilip Kumar Yadav, " RSA and ECC: A Comparative Analysis ",International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017)

[14] Snehal Jawanjal, Shrikant Bhoyar, " Review paper on Reed Solomon (204,188) Decoder for Digital Video Broadcasting – Terrestrial application", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 03 Issue: 01,2016.

[15] Priyanka Shrivastava, Uday Pratap Singh, " Error Detection and Correction Using Reed Solomon Codes", Volume 3, Issue 8,2017