ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

# Secret Data Hiding Using ECDSA Algorithm

Mrs.M.Meenalochini[1], M.Amutha[2], R.Gokilapriya[3], S.Mythili[4], S.Nageswari[5].

Assistant Professor, Jai Shriram Engineering College, Tirupur, Tamil Nadu, India. [1]

UG Scholar, Jai Shriram Engineering College, Tirupur, Tamil Nadu, India. [2,3,4,5]

**ABSTRACT:** This project proposes the enhancement of security system for secret data communication through encrypted data embedding in fingerprint images. A given input image is converted to any one plane process and encrypted by using elliptic curve digital signature encryption. After plane separation, the encrypted data hider will conceal the secret data into the image pixels. The secret data hiding technique uses for concealing the secret message bits into the encrypted image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the image pixels to extract the data. By using the decryption key, the data will be extracted from Input image to get the information about the data.

**KEYWORDS**: Fingerprint image, data hiding, ECDSA, security.

## I. INTRODUCTION

Computer and internet are the major media that connects different parts of the world as one global virtual world in this modern era. That's why we can exchange lots of information easily at any distance within seconds of time. But the confidential data need to be transferred should be kept confidential till the destination. Rapid enlargement in number of attack recorded during electronic exchange of information has certainly called for more robust method for securing data transfer. Information security has grown as a prominent issue in our digital life. The network security is becoming more significant as the volume of data being exchanged over net increases day by day. One of the reasons why attackers become successful in intrusion is that they have an opportunity to read and understand most information from system. The most important motive for attacker to benefit from intrusion is value of confidential data he can obtain by attacking the system. Hackers may expose the data, alter it, distort it or employ it for more difficult attacks. The solution for this problem has led to the development of cryptography and steganography. By combining cryptography and steganography in one system we can ensure enhanced security.

Cryptography and steganography is not capable of protecting the data alone. To improve information security and to maintain secrecy and privacy of data, steganography and cryptography alone is not sufficient. Cryptography can be used where steganography is inefficient and steganography can be used where cryptography is inefficient. Thus a new approach of combining both techniques has been proposed by many researchers for secure storage and transmission of data.

## II. BACKGROUND DETAILS

### A. Cryptography

Cryptography is one among many aspects of building security. It is a powerful tool used to protect information in computer systems. When we use the browser for home banking we use a number of cryptographic algorithms for protecting the confidential data. Even the computer passwords are protected by cryptographic hash functions. When we send an email, it is also encrypted by SSL. Modern cryptography concerns itself with confidentiality (information cannot be processed by anyone for whom it was not intended), integrity (information cannot be altered), and authentication (sender and receiver can confirm their identity).The aim of cryptography is to store and transmit data in a particular form so that only those for whom it is intended can read and process it. To achieve this data is scrambled into cipher text, an unreadable format.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Cryptographic system can be classified based on,
1) Methodology for transforming plain text to cipher text: It includes substitution technique and transposition technique. In substitution technique, plain text is mapped into another element and in transposition technique, plain text is rearranged.
2) Methodology for number of keys used : It includes secret key cryptography, public key cryptography and hash function. Secret key cryptography method employs a single key for both encryption and decryption. The sender uses a key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Since a single key is used for both function, this cryptography is also called symmetric key cryptography. This is faster compared to asymmetric key cryptography. Here the keys must be known to both sender and the receiver. The difficulty of this approach is the distribution of the key. The secret key cryptographic algorithm in use today includes DES, AES, CAST-128/256, Blowfish, Rivest cipher etc.
3) Methodology for processing plain text: In block cipher technique processing or encoding of the plain text is done as a fixed length block one by one. A block example could be 64 or 128 bits in size. The same key is used to encrypt each of the blocks. A pad is added to short length blocks. It is usually more complex and slower in operation and examples of block cipher are Lucifer, IDEA, RC5 etc.

**B. Steganography**

Steganography derived from 2 Greek words ‘steganos’ which means either secret or covered and ‘graphein’ which means writing or drawing. In this case steganography literally means covered writing. The Greeks would actually use this method to transmit secret messages more than 2000 years ago. Normally in those days they wrote on tablet covered with wax. The first recorded use of the word steganography came up from 15th century book called steganographia, disguised as a book on magic. This was written by Johannes Trithemius. Steganography means hiding a secret message within another message. In digital computing there are many opportunities for steganography. Steganography is the practice of concealing information or files within non secret data. The file containing the secret data is called the carrier. The modified carrier looks like original carrier. Best’s carriers are images, audio, video files since everybody can send receive download them. Steganography is not encryption. The data is hidden not encrypted.

Steganography techniques can be generally classified as,
1) Spatial domain technique: In spatial domain steganography bits in the pixels values are changed in order to hide the data. Spatial domain techniques can be classified into Least Significant Bit (LSB), Pixel value Differencing (PVD), Random Pixel Embedding method, histogram Shifting method, Texture Based method etc. LSB is the widely used simplest method where there is less chance for degradation of original image.
2) Transform domain technique: Transform domain embeds information in transform space. In this domain, the image is transformed from spatial domain to frequency domain by using any transforms and after a transformation process, the embedding process will be done in proper transform coefficients. The process of embedding data in the frequency of a signal is much stronger than embedding principles that operate in the time domain.
3) Distortion technique: This technique store message by distorting the cover slightly and detecting the change from the original. The decoder function uses the original cover image during decoding process to find the difference between original and distorted cover image in order to restore secret message.
4) Masking and filtering: This technique is usually restricted to grayscale and 24-bit images. It doesn’t hide the data in noise level but embeds it in significant areas. Masking adds redundancy to the hidden information. This method is more robust than LSB modification with respect to compression and different kinds of image processing since the information is hidden in the visible parts of the image

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

## III. RELATED WORK

**Quality measures for image**

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance $\sigma_q^2$. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} ( f[j,k] - g[j,k] )^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{MSE} \right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

Correlation Coefficient: It is used to find the similarity between two different images with their intensities. It will be described by,
Cor_coef = [sum(sum(u1.*u2))] / [sqrt(sum(sum(u1.*u1))*sum(sum(u2.*u2)))];
Where, u1 = F1 – mean of F1, u2 = F2 – mean of F2
F1 – Cover Image and F2 – Encrypted Image

**ECDSA Key Generation**

The user A follows these steps where p is a large prime:

- Select a random integer d ∈ [1, n - 1].
- Compute Q = d x P.
- The public and private keys of the user A are Q and d, respectively.

The other parties can check if the public key is valid by;

- Checking that $Q \neq 0$.
- Checking that $x_Q$ and $y_Q$ are properly represented elements of $F_q$.
- Checking that Q is on the elliptic curve defined by a and b.
- Checking that nQ = Q.

If any of these checks fail the public key Q is invalid, otherwise Q is valid. The following procedure describes how to generate the signature

**ECDSA Signature Generation**

The user A signs the message m using the following steps as shown in Fig. 1.

- Select a pseudorandom integer k ∈ [1, n - 1].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

- Compute k x P = $(x_1, y_1)$ and r = $x_1$ mod n.
  If $x_1 \in GF(2^k)$, it is assumed that $x_1$ is represented as a binary number.
  If r = 0 then go to Step 1.
- Compute $k^{-1}$ mod n.
- Compute $s = k^{-1}(H(m) + d \bullet r)$ mod n.
  Here H is the secure hash algorithm SHA-1.
  If s = 0 go to Step 1.
- The signature for the message m is the pair of integers (r, s).

**ECDSA Signature Verification**

The user B verifies A's signature (r, s) on the message m by applying the following steps as shown in Fig.2

- Compute $c = s^{-1}$ mod n and H(m).
- Compute $u_1 = H(m) \bullet c$ mod n and $u_2 = r \bullet c$ mod n.
- Compute $u_1 \times P + u_2 \times Q = (x_0, y_0)$ and $v = x_0$ mod n.
- Accept the signature if v = r.

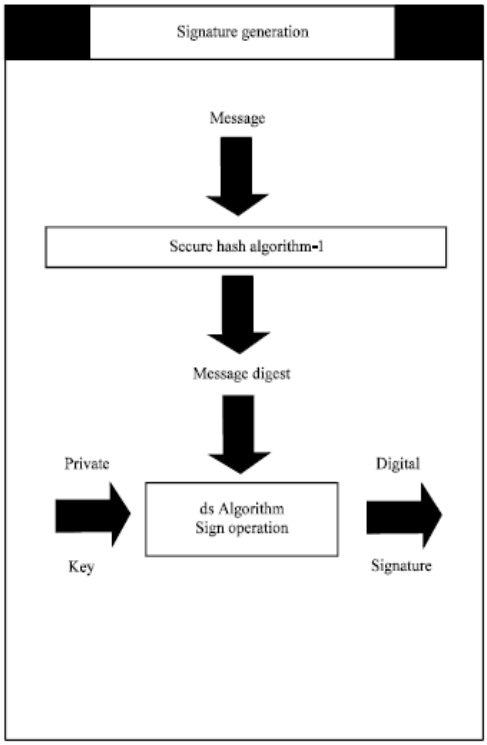



Fig 1: Signature generation schematic

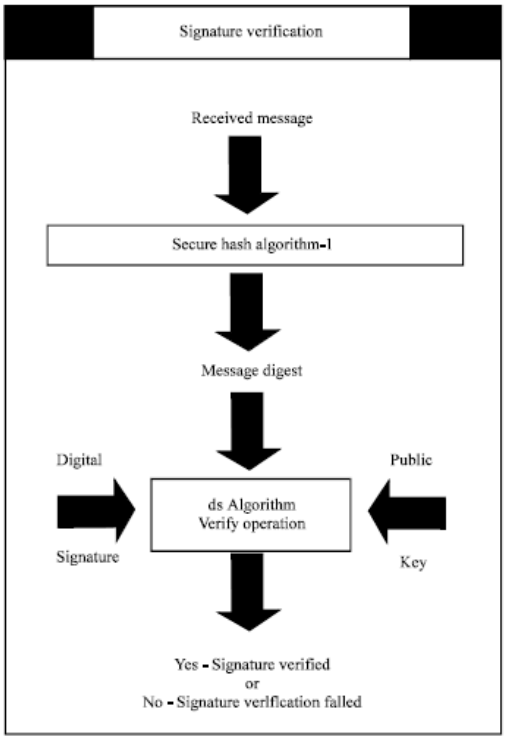



Fig 2: Signature verification schematic

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

## IV. SOFTWARE IMPLEMENTATIONS

### MATLAB

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. Typical uses include:

- Math and computation
- Algorithm development
- Modeling, simulation, and prototyping
- Data analysis, exploration, and visualization
- Scientific and engineering graphics Application development, including graphical user interface building

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non interactive language such as C or FORTRAN The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects. Today, MATLAB uses software developed by the LAPACK and ARPACK projects, which together represent the state-of-the-art in software for matrix computation.

MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis. MATLAB features a family of application-specific solutions called toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and apply specialized technology. Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes of problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

## V. EXISTING SYSTEM

It generates the fingerprint image based on a piece of hologram phase constructed from the secret message. The hologram phase consists of the spiral phase and the continuous phase. First to map the secret message to a polynomial and encode it into a set of points with different polarities, from which the spiral phase is computed and constructed. Then, construct the continuous phase by decomposing a fingerprint image synthetically generated. The spiral phase and the continuous phase are combined to form the hologram phase. This is eventually used to construct a fingerprint image in a common form such as the grayscale fingerprint image, binary fingerprint image, or thinned fingerprint image. The secret message can be extracted by detecting the encoded points in the constructed fingerprint. By constructing fingerprint images with ordinary sizes, the results show that the secret message can be extracted accurately. It is also difficult to detect the existence of secret message from the constructed fingerprint images.

## VI. PROPOSED SYSTEM

Data and Information Security has become very important in today's modern world, as a result of these various methods are adopted to bypass it. With the advent of the internet, security has became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The mechanism of the internet, when modified can reduce the possible attacks That can be sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many modern spare secure themselves from the internet by means of Elliptic Curve Cryptography, Text Encryption and Decryption process and Card Shuffling Process. It provides higher level of security with lesser key size compared to other Cryptographic techniques. A new technique has been proposed in this paper where the classic technique of mapping the characters to affine points in the elliptic curve has been removed. The corresponding ASCII values of the plain text are paired up. The paired values serve as input for the Elliptic curve cryptography. This new technique has

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

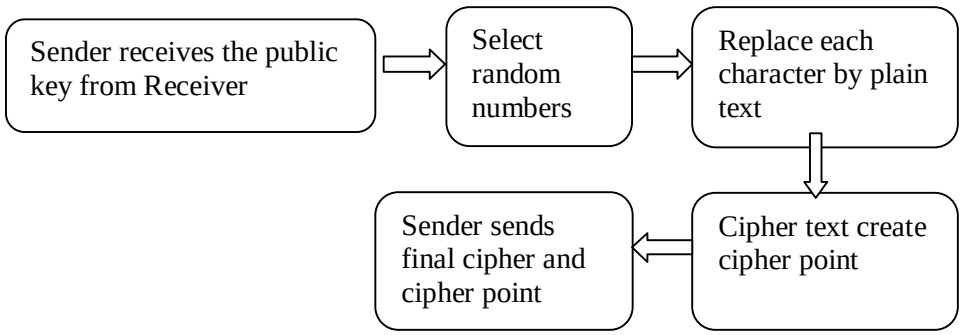
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

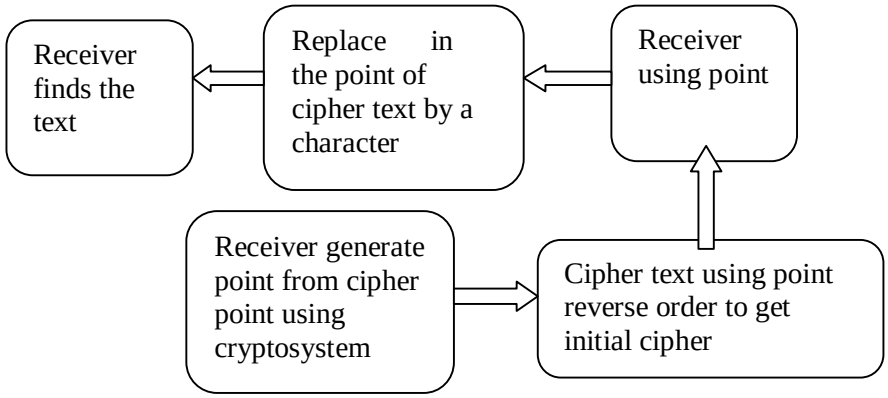
Vol. 7, Issue 2, February 2019

been avoided for the costly operation of mapping and the need to share the common lookup table between the sender and the receiver. The algorithm is designed in such a way that it can be used to encrypt or decrypt any type of script with defined ASCII values. Cryptographic algorithms are available publicly, though some organizations believe in having the algorithm a secret. The general method is in using a publicly known algorithm while maintaining the key secret. We have studied Application of Elliptic Curves over card shuffling logic for traditional key exchange and encryption of text. We have implemented both and proposed a scheme for encryption of images. It was partially accomplished for a small size image.

**ENCRYPTION:**




**DECRYPTION:**




## VII. CONCLUSION AND FUTURE WORK

Elliptic Curve Digital Signature Algorithm (ECDSA) which is one of the variants of Elliptic Curve Cryptography (ECC) proposed as an alternative to established public-key systems such as Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA), have recently gained a lot of attention in industry and academia. The main reason for the attractiveness of ECDSA is the fact that there is no sub-exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. Hence, it takes full exponential time to solve while the best algorithms known for solving the underlying integer factorization for RSA and discrete logarithm problem in DSA both take sub-exponential time. The keys generated by the implemented software is highly secured and it consumes lesser bandwidth because of small key size used by elliptic curves and this is also coupled with the introduction of open source software into this work, which is generally believed to be more secured than those traditionally available on closed source operating systems like Microsoft Windows. Significantly smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA, but with equivalent levels of security. Some benefits of having

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

smaller key sizes include faster computation time and reduction in processing power, storage space and bandwidth. This makes ECDSA ideal for constrained environments such as pagers, personal digital assistants (PDAs), cellular phones and smart cards. These advantages are especially important in other environments where processing power, storage space, bandwidth, or power consumption are lacking. The above properties makes communication to be more secure on the internet hence making electronic business and other transactions to be carried out with little or no fear of hackers.

## REFERENCES

[1] JidagamVenkataKarthik, B.Venkateshwar Reddy, "Authentication of Secret Information in Image Steganography", International Journal of Latest Trends in Engineering & Technology, ISSN: 2278-621X, Vol. 3(1), Sep 2013, pp. 97-104.
[2] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010, pp. 3-6.
[3] Shristi Mishra, Prateeksha Pandey "A Review on Steganography Techniques Using Cryptography", International Journal of Advance Research In Science And Engineering, Vol. No.4, Special Issue (01), March 2015
[4] MoreshMukhedkar, PrajktaPowar and Peter Gaikwad, "Secure non real time image encryption algorithm development using cryptography & Steganography", IEEE INDICON, 2015.
[5] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, 2010. (Auerbach, Sept. 1998).
[6] Vipul Shanna and Madhusudan "Two New Approaches for Image Steganography Using Cryptography" IEEE Int. Conf. Image Information Processing, 2015.
[7] Kamaldeep Joshi, RajkumarYadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP, 2015.
[8] Mehdi Hussain and MureedHussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013.
[9] K.S. Seethalakshmi, Usha. B, Sangeetha. K. N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", IEEE Int. Conf.Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.
[10] SadafBukhari, Muhammad ShoaibArif, M.R. Anjum, and SamiaDilbar, "Enhancing security of images by Steganography and Cryptography techniques", IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016