HYBRID TECHNIQUE FOR HIGH PAYLOAD CAPACITY USING ECC AND STEGANOGRAPHY.

Sai Deepak Tatavarthi¹, Vamsidhar Enireddy²

¹M. Tech Student, Department of CSE (Cyber Security and Digital Forensics), Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, deepaktatvarthi1997@gmail.com
²Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, entreddy.vamsidhar@gmail.com

ABSTRACT

Information plays crucial role in any organization in this present generation usage of internet and generating lots of information is increased exponentially. To protect this information is a big challenge for every organization. For suppose while storing the data on cloud we must face many problems like data confidentiality, integrity, availability. To provide the solution for this problem have a different data security technique one of the most popular is Cryptography and another one is Steganography. Number of papers are published with these techniques but, this paper proposed a hybrid security for information using different algorithms and providing better security to information and achieving high payload capacity.

Keywords: Cryptography, ECC Algorithm, Steganography, LSB Technique, Bitwise Operator

I. INTRODUCTION

Now a day’s cloud computing technology is very useful in our present day to day life and also many areas like industry, military, colleges etc, to store their huge amount of data. The central remote servers provide and maintain the data of users and they provide the access on the internet. The data can be stored by medical professional, patients for their understanding, government authorities and insurance companies etc. Medical related data can be secured in the form of Electronic Health Records these are available online at any time. These records contain data like scan images, medical prescription, patient information. No doctor can be stored patient information in the form of paper format. These cloud service providers are not providing complete security to user’s data because of they are giving to services as very low cost. While storing the data on cloud we must face many problems like data confidentiality, integrity, availability. To provide the solution to these problems there are n number of methods. To provide data security Cryptography and Steganography techniques are more popular now a days [1].

![Cryptography Process](image)

Fig-1: Cryptography Process
Cryptography is the process of changing data from plain text to cipher text which is human unreadable format. It is used for security purposes to protect valuable data. The sender encrypts the data using algorithms and sends it to the receiver, who must decrypt the cipher text using the algorithm and valid key. The receiver must reverse the encryption process to obtain the original plain text. Cryptography is used for secure communication against insecure channels. There are two types of cryptographic techniques available to secure the data: symmetric and asymmetric key-based algorithms. In the above figure 1 shows how the cryptography process works:

Non-repudiation means the sending person sends the information which cannot be denied at a later stage. The sender’s intention while sending information is non-repudiated.

In literature, several research articles are found in cryptography. FPGA-based random generators are used for communication [12,13]. To provide security for the data in IoT devices, lightweight cryptography algorithms are used [14]. A new watermarking technique is implemented to provide health care images that cannot be compressed to occupy less space [15]. DNA-based cryptography with the OTP generation is implemented for providing better security [16]. Stochastic and homomorphic key generation mechanisms are introduced in cryptography for various applications [17,18]. ECC-based cryptography algorithms are used for random key generation and also Verilog-based encryption and decryption of 8-bit data is also implemented based on the ECC algorithm [19,20].

**Symmetric key cryptography:**

In symmetric key cryptography, both encryption and decryption use the same key. The same key is used for encryption at the sender side and decryption for the receiver side. If anyone gets the key, then easily get the whole encrypted data without any difficulty. This technique is called single key cryptography, private key cryptography, shared key cryptography, secret key cryptography. Examples: DES, 3DES, AES, RC4, BLOWFISH algorithms [21].

**Fig-2: Symmetric Cryptography**

**Asymmetric Key cryptography:**

In asymmetric key cryptography, two different keys (public key, private key) are used. The public key is used at the sender side for encryption, and the private key is used for decryption at the receiver side. Anyone can use their public key for encryption at the sender side, but only the receiver or authorized person can decrypt the message as their private key. The main thing is only authorized persons can decrypt the message, whereas symmetric anyone can decrypt who have the private key. Example: RSA, ECC, ELAGAMAL Algorithms [2].
Hash Function:
Hash function is a function it is generating unique hash value for input data for integrity purpose. Example: MD5, SHA-1, MD2, MD4, SHA-256, SHA-512.

Fig-4: Hash Function

CYBER ATTACKS ON CLOUD:
Cyber-attacks performed on cloud and causes various serious harms. The main goal of cyber-attack is to steal the sensitive information of user’s whatever data stored on cloud. So, this case cloud service provides takes necessary action to protect the user’s data. These are some most common attacks on cloud computing [3]:

- Denial of service attacks (DOS)
- Man-in the Middle attack
- Insider Threats
- Broken Authentication attack
- Crypto jacking
- Malware injection attack

II. STEGANOGRAPHY
The term steganography refers to the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection.

Methods of steganography
- Audio-based steganography
- Image-based steganography
- Video-based steganography
• White text Steganography

Steganography is the practice of hiding a file, message, image or video in another file like message video or audio. In general, the hidden message seems like something else like pictures, articles and sometimes shopping list. While the practice of encryption is to protect the content of a message alone, the style of steganography both concerns the disclosure and content of a secret message. Steganography covers data concealed in computer files. So, let us understand this in a better way with the examples.

**Purpose of Steganography**

Effective communication is steganography. At first, you can encrypt and hide a private file inside a picture of another file type before sending it to somebody else. The likelihood of being intercepted will reduce. If you send any encrypted file to someone the other person will try to decrypt it in many ways and possibly, he will be able to do so. But in this case, it will reflect like a normal image and the other person will have no hint that what can be there on the other side of the picture. So, it is always a better and safe way of communication for those organization’s where they want to protect their selves from these kinds of attacks.

In this paper we are using image to image steganography since image to image and text to image steganography both are same

**Evaluation of image steganography**

Three parameters must be considered when applying steganography technique those are security, imperceptibility, Capacity. If you are achieving these three parameters, then only we can say that is good steganography, but we cannot achieve all these at a time.

If we want to provide better security, we cannot store more information because let us take LSB Technique we are storing bits from left most bit to right most bit if bit position will increase from left to right the stego image quality should be distorted then attacker can easily predict there is something behind that stego image.

If we could not store huge information, we can achieve better security because of stego image quality wont distorted. So, to solve this problem many researchers are keep on trying to get good solution that is achieving both parameters like by combining two different techniques or by modifying existing techniques and soon [4].

![Fig-5: Evaluation Parameters](image)

**Elliptic curve Cryptography (ECC):**

ECC provides greater data security on a input key size, Even if the key size is small it gives better security and mainly ECC consumes less computing power and

Less heat creation. We know the small keys makes speed up the cryptographic functions, because of process runs on smaller chips. There are various kinds of reason to select this algorithm:

1) Less computing power and less heat generation.

2) For a given key size ECC provide greater security.

3) Practically not possible to identify private key so no third person cannot inspect the secret key.
In this algorithm encryption and decryption are very fast compare to other algorithms and it uses small keys especially public cryptosystems and provides same level of security [5]. Elliptic curves are defined to perform encryption or decryption we need to use different elliptic curves. Those are Elliptic curve over prime numbers (Zp), real numbers and finite field (GF). Elliptic curve uses cubic equations, and the cubic equation is defined as:

\[ y^2 = x^3 + ax + b \]

To plot a curve, we have to compute y value from this equation \( Y = \sqrt{x^3 + ax + b} \) for every a and b. Here Y will generate +ve and -ve value then the line is symmetric \( y = 0 \) and we will get x values as well.

Before going to encryption and decryption with that (x, y) values we have to identify some of the rules for addition.

We have plotted a curve with that above cubic equation if any their points make a straight line then the sum of three points as zero. Now zero act as identity element.

\[ P + 0 = P, \]

If point \( P (x_p, y_p) \) the negative of p represented as \(-P (x_p, -y_p)\).

To perform ECC we are using Diffie Helman Key Exchange concept.

Let us take plain text \( P_t (x, y) \) to perform encryption or decryption we required an elliptic curve over G, \( E_q (a, b) \) elliptic group parameters and random integer K.

Encryption

\[(\text{Cipher Text}) = \{KG, P_t + KP_b\}\]

Where as \( P_b \)is public key of receiver.

Decryption

\[(\text{Plain Text}) = \{P_t + KP_b - (N_b * KG)\}\]

Whereas \( N_b \)is private key of receiver.

In this way we are going to encrypt the plain text using ECC algorithm with Diffie Helman Key Exchange [6].
III. EXISTING SYSTEM

Many papers have been proposed in this method. For providing security the author first encrypting the secret image with any cryptographic algorithm then we will get ciphered image after that embedding cipher image bits behind cover image then finally generates stego image. In this case for the purpose of distorting the cover image the authors can be embedding less information but providing better security. In this era lots of internet users are increased and generating huge amount of data sometimes we should store huge amount of data with less security at that case our proposed model will be very helpful [7].

Drawback:
- Less Payload Capacity
- Less Secured

IV. PROPOSED SYSTEM

In this proposed model we are focusing to increase payload capacity as much as possible, here first we are taking an image as cover image. And read every pixel in image convert it as decimal to binary for RGB pixels and store it as in place.

Here encrypting cover image instead of secret image with strongest and secure cryptographic algorithm which is ECC and with rand key generation it gives us Ciphered image. This image cannot understand by human. After encrypting cover image, we will get cipher image so we can embed more information because of cover image already distorted.
Then we have covered image with us next step to take the secret image for embedding secret information into cover image.

Now with this secret image we are going to store this behind covered image this concept we call it as steganography and if we want to increase security instead of placing secret information, we will place bits by applying XOR operation with secret images bits and cover image then result stored in cover image itself. Like same as cover image, we convert each pixel of secret image into binary format then only we can do the XOR operation and interchange the bits. Finally, we will get this embedded secret image.

With this embedded image we are going to reconstruct as original cover image using DCT method [8].
Finally, we will get as cover image then this will send to receiver through any secure transmission medium.

For retrieving secret information, we will do reverse engineering as reverse process of encoding process.

The below steps are explained clearly how the proposed model is working.

V. ENCRYPTION

Step 1: First read the cover image.

Step 2: Apply ECC Algorithm for every pixel in cover image we will get output as ciphered image.

Step 3: Select secret image and take every pixel of binary bits apply XOR Operation with Cover image pixel binary bits and embedded with cover image bits from left to right [9,10].

Step 4: Finally, we will get the embedded secret information of ciphered image.

Step 5: We need to reconstruct the stego image into cover image. Then send to cloud.

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P ⊕ Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Fig-14: XOR Truth Table

The Decryption process same as reverse of encryption process. We must provide the security, high payload capacity, and imperceptibility when we are dealing with steganography and these three can be necessary while data is transmitting one place to another and data at stored in servers.

With this proposed model we can achieve all the steganography Evaluation parameters.
VI. EXPERIMENTAL RESULTS

Histogram describes that the graph whose x-axis and y-axis of the pixel difference of each pair. It is used to identify the differences in between cover image and stego image. Cover image and Stego image will be compared to monitor any shapes or any pixel distribution for any steganographic algorithm [11].

VII. CONCLUSION

Cryptography and Steganography are most powerful techniques to secure data from attackers. Whenever you want to transfer or store the data you must be provide security. In this proposed scheme we have used hybrid method to provide better security and to increase the embedding information capacity we implemented new method which is to encrypt the cover image. This method will helpful when the data must be stored securely. Hence the proposed system is resistant to statistical and dynamical attacks, high speed and robust to noise and loss of information.

REFERENCES:


www.turkphysiotherrehabil.org

