**Modelling Novel Secure Technique for Handling Threats**

***Ms. Sahaana Iyera, Ms. Praditi Redeb, Ms. Sheetal Sharmac, Prof.Sunil Chaudharid***

*a,b,c,d (Computer Engineering Department, Fr. Conceicao Rodrigues COE, Mumbai, University of Mumbai )*

*a sahaanaiyer@gmail.com*

*bpraditi.rede@gmail.com*

*csharmasheetal9798@gmail.com*

*dexample@example.com*

**ABSTRACT**

A novel technique for generating a new security framework and dealing with security threats based on a combination of cryptography and steganography. Cryptography keeps the contents of the message secret by converting the actual data into cipher data by encrypting it, while steganography embeds the message into the cover image. There are a variety of cryptography techniques available, out of which AES is the most secure technique for encrypting the data. The steganography technique hides the encrypted data in image so the message is secured. In Cryptography the message is encrypted using the AES algorithm and part of the message is concealed in an image DCT using steganography technique. The keys are shared using Diffie-Hellman Key Exchange Algorithm for secure transfer of keys.

*Keywords: Cryptography, Steganography, Advanced Encryption Standard (AES), Diffie-Hellman Key Exchange Algorithm, Discrete Cosine Transform (DCT), Stego Image, Data Security.*

**1. INTRODUCTION**

Cryptography, which encrypts plain text to produce ciphertext, is a popular method of securing communication. The transmission of ciphertext, on the other hand, can easily arouse attackers' suspicions, and the ciphertext can thus be violently intercepted, struck, or decrypted. In recent years, steganography has been established as a modern clandestine communication method. Cryptography is classified into two types based on the number of keys used. There are two types of encryption techniques: private key encryption and public key encryption. Private key encryption techniques use the same key at both the sender and the receiver, whereas public key encryption techniques use two different keys, one for encryption and the other for decryption. Encryption scrambles data so that an unauthorized receiver can't figure out what it's for. Steganography, on the other hand, attempts to prevent an unintended recipient from suspecting the presence of data.

**2. BACKGROUND THEORY**

In recent years, image steganography has attracted considerable research and popular utilisation in comparison with other types of steganography.This is due to the fact that large volumes of data can be obscured without causing any significant impact on the carriers, as well as the widespread availability of electronic images. Steganography alone is at risk of attackers. When steganography and cryptography are combined, we get better results.

***2.1 Advanced Encryption Standard (AES)***

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

AES performs all its computations on bytes rather than bits. AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. Each round comprises four sub-processes - Byte Substitution (SubBytes), Shiftrows, MixColumns, Addroundkey. The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

***2.1.1 Advantages of using AES***

Very Secure, Reasonable Cost, Flexible, Simple.

***2.2 Diffie-Hellman Key Exchange Algorithm***

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.This algorithm can be used only for key agreement, but not for encryption and decryption.

First, we define a primitive root of a prime number pas one whose power generate all the integers from 1 to (p-1) i.e., if „a‟ is a primitive root of a prime number p, then the numbers a mod p, a2 mod p, … ap-1 mod p are distinct and consists of integers from 1 to (p-1) in some permutation. For any integer „b‟ and a primitive root „a‟ of a prime number „p‟, we can find a unique exponent „i‟ such that b ≡ ai mod p where 0 ≤ i ≤ (p-1).The exponent „i‟ is referred to as discrete logarithm.

***2.2.1 Advantages of using Diffie and Hellman algorithm***

Sharing of keys is done securely.

***2.3*** ***DCT (Discrete Cosine Transform) - frequency domain algorithm for Steganography***

The message is inserted into the DCT domain of the host image. To insert the secret message into the DCT domain of the cover picture, the hidden message is a stream of “1” and “0” with a total of 80 bits. The transform is applied to the image as a multiple factor of 8x8 blocks.Then, in the low-mid frequency range, at least 80 larger positive coefficients must be embedded in the cover picture.The image details are represented by the high frequency coefficients, which are vulnerable to most common image manipulations such as filtering, compression, and so on.The low and mid frequency coefficients are the most suitable for this work because the key problem is robustness against high image quality.The coefficients selected here are ordered by magnitude, then modified in the message stream by the corresponding bit. A quantity D is applied to the coefficient if the ith message bit s(i) to be embedded is "1."This D quantity represents the persistence factor.The same number is removed from the coefficient if the message bit is "0."Thus the replaced DCT coefficients are:-

DCT (new) = DCT+1\*D for s(i)=1;

Else DCT (new) =DCT-1\*D for s(i)=0

***2.3.1*** ***Advantages of using DCT - frequency domain Steganography***

1. Extremely secure, difficult to detect

2. More adaptable and diverse techniques for calculating DCT coefficient values.

**3. PROPOSED TECHNIQUE**

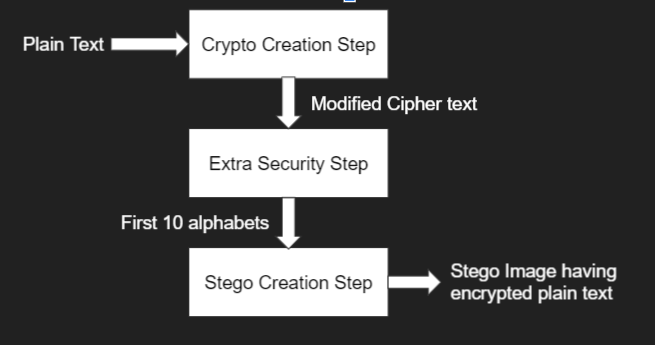
The proposed system is divided into following steps:-

1. For Cryptography – Crypto Creation Step.
2. For Extra Security – Security Creation Step.
3. For Steganography – Stego Creation Step.

In cryptography, the system employs the AES algorithm with its symmetric key which is generated from Diffie-Hellman Key Exchange Algorithm and the cypher text is converted into hexadecimal format. Two extra keys are generated by the Security step for additional security, after which steganography is applied to the key to obtain the stego image. The process flow for hiding and retrieving the text is as follows-

***3.1 Hiding the Text***

The steps for hiding the test are as follows (see Figure 1):

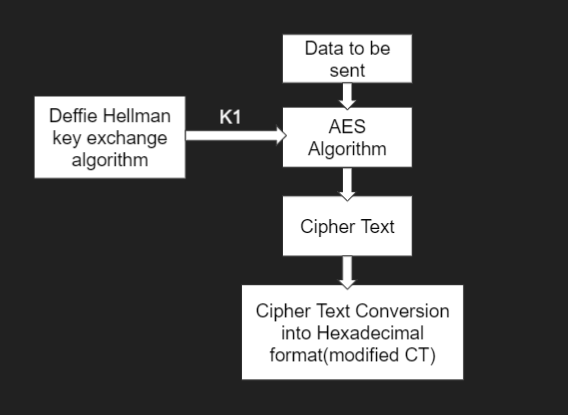
******

*Figure.1 Hiding the text*

***3.1.1 Crypto Creation Step***

The steps for encrypting data in the Crypto Module are as follows (see Figure 2):

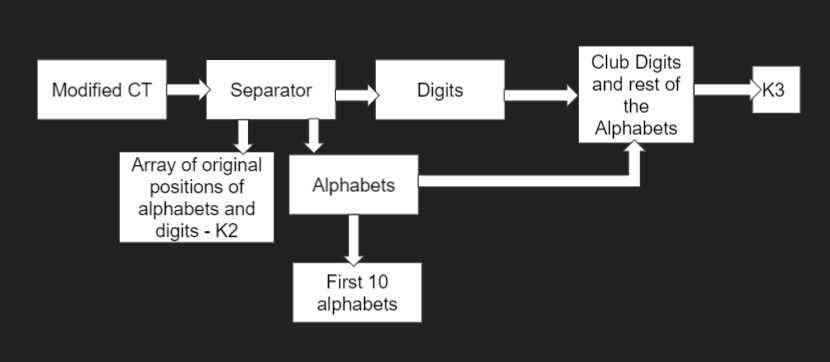
* Enter the text to be encrypted.
* Generate the Key-K1 for encryption of the text using Diffie-Hellman Key Exchange Algorithm.
* Use the AES algorithm with a 128-bit key to encrypt the text.
* Convert the ciphertext into Hexadecimal format

*Figure.2 Crypto Creation Step*

***3.1.2 Security Creation Step***

The steps for creating extra security are as follows (see Figure 3):

* Keep the track of original position of alphabets and numbers in modifies cipher text (cipher text converted in hexadecimal format) alternatively in Key - K2 (if number of Alphabets is not equal to number of Numbers place larger in sequence at last)
* Seperate the alphabets and digits from the modified cipher text.
* Separate first 10 alphabets from the modified text.
* Club the digits and remaining alphabets in Key-K3.

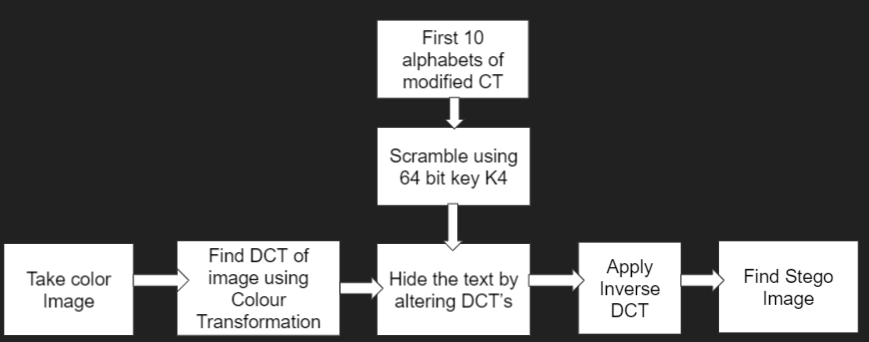


*Figure.3 Security Creation Step*

***3.1.3 Stego Creation Step***

The steps for creating Stego Image from result of security creation step are as follows (see Figure 4):

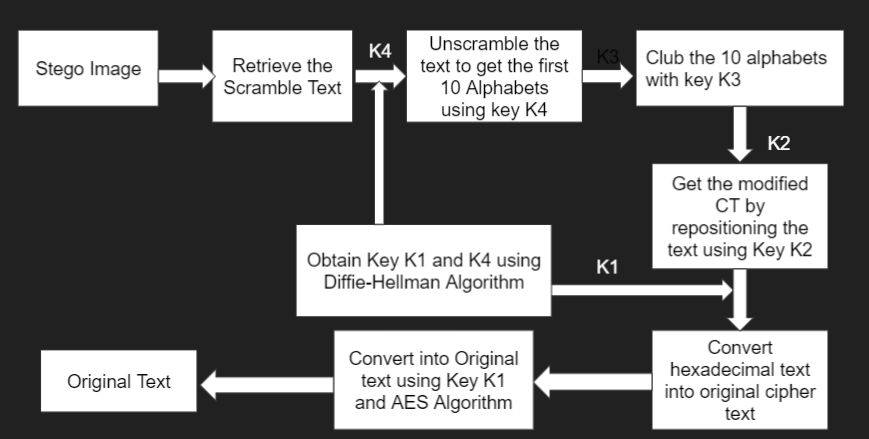
* Scramble the first 10 alphabets generated in the security creation step using a 64 bit Key K4(Key is generated using Diffie-Hellman Key Exchange Algorithm).
* Take a Color Image.
* Find the DCT of the Image using color transformation.
* Hide the Cipher by altering DCTs.
* Apply Inverse DCT.
* Find the Stego Image

*Figure.4 Stego Creation Step*

***3.2 Retrieving Text***

The steps for retrieving text are as follows (see Figure 5):

* Generate the Keys K1 and K4 using Diffie Exchange Key Exchange Algorithm.
* Get the scrambled text out of the stego image.
* Unscramble the text with key K4 to get first 10 alphabets.
* Combine the 10 alphabets with key K3 To get the entire text.
* To obtain the modified CT, reassemble the text using original positions stored in key K2.
* Transform the hexadecimal text into the original ciphertext.
* Convert into original text using Key K1 and AES Algorithm.



*Figure.5 Retrieving Text*

**4. CONCLUSION**

Using two keys and modified cipher text, this study proposes a modern digital message hiding scheme that combines cryptography and steganography. The combination of these two strategies meets criteria such as sender and receiver protection and robustness. Steganography, particularly when combined with cryptography, is a powerful tool that allows people to communicate without eavesdroppers even being aware that they are communicating. The proposed method ensures acceptable image quality with very little distortion in the image. The main advantage of this approach is that the AES algorithm is extremely stable, and the DCT transformation technique is extremely difficult to detect in image steganography. The purpose of this paper is to develop a new safety system that any attacker or hacker in the communication process cannot retrieve messages easily from the image.

**5. REFERENCES**

[1]B.Raja Rao, P.Anil Kumar, K Rama Mohana Rao, M.Nagu, “A Novel Information Security Scheme using Cryptic Steganography”, B. Raja Rao et. al. / Indian Journal of Computer Science and Engineering Vol. 1 No. 4 327-332

[2]Dipti Kapoor Sarmah, Neha Bajpai, “Proposed System for Data Hiding Using Cryptography and Steganography”, International Journal of Computer Applications.(0975 – 8887)

[3]Lokesh Kumar,”Novel Security Scheme for Image Steganography using Cryptography Technique”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012

[4]Smt. K. Venkata Ramana, Smt.S. J. R. K. Padminivalli. V, Ms. V. Vijaya Lakshmi, “A Novel Technique for Secure Data Transmission using Distributed Steganography and Cryptographic Techniques”, International Journal of Engineering Research & Technology (IJERT) Vol. 4 Issue 02, February-2015

[5]Pye Pye Aung, Tun Min Naing ,”A Novel Secure Combination Technique of Steganography and Cryptography”, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No. 1, February 2014

[6] Kharrazi, M., Sencar, H. T., and Memon, N. (2004), “Image Steganography: Concepts and practice.” In WSPC Lecture Notes Series

[7] William Stallings, “Cryptography and Network Security: Principles and practices‖, Pearson education”, Third Edition, ISBN 81-7808-902-5