International Journal of Computer Architecture and Mobility
(ISSN 2319-9229) Volume 1-Issue 8, June 2013

Analysis of Triple DES and RSA Algorithm in securing Image Steganography

Megha Zodape
(M.E. student)
IET,DAVV Indore
meghazodape@gmail.com

Mrs. Pragya Shukla
Associate Professor
IET,DAVV Indore
pragyashukla_iet@yahoo.co.in

Abstract:
Image Steganography is an art of hiding information in the image in such a way that the attacker will not able to realize the existence of data in the image. Image steganography is being used widely after it has been introduced. The techniques used for hiding information in the image is common and is based on using Least Significant Bit for storing information bit. As the technique is known to all, the attacker will be able to easily reveal the information, this makes image steganography unsecured. In order to increase the security of image steganography can be combined with cryptography, so that even if the attacker knows the hiding method will not able to reveal the information. This paper presents the performance analysis of two most important cryptography algorithms, Triple DES and RSA when used along with image steganography.

Keywords: cryptography, steganography, ciphertext, stego image,RSA,LSB,Triple DES,steganalysis,cover image,

Introduction:
In steganaography the information is hidden in the media like text, image, audio and video. It is different from cryptography as it conceals the existence of information whereas cryptography only changes the form of information making it unreadable for an attacker. In image steganography the information is hidden in the image in such a way that it does not make greater changes in the appearance of the image. The schematic diagram is shown in the fig1 and fig2

Sender Side

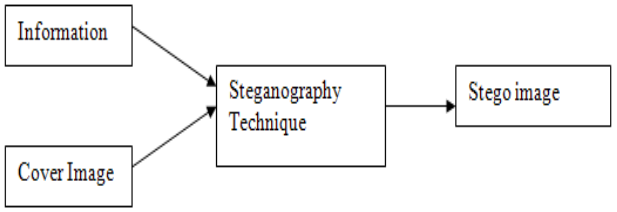


Fig:1

Receiver Side

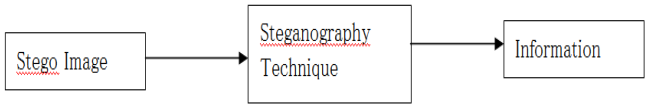


Fig:2

Fig:1 shows the sender side of a steganography technique,the information is hidden in the cover image by using steganography technique
Fig:2 shows the receiver side where a stego image is taken and reverse steganography technique is used to retrieve information .

The technique used for hiding the information is based on LSB method. In this method the LSB of each color of pixel is stored in a file. The file is then traversed to find the same pattern as of information bit and the location of the pattern is noted. If same pattern is not found the best matched bit pattern of the file is searched and replaced with the information bit and location is stored in file. This makes minimum changes in the cover image.

Given two identical image, if the least significant bits of the pixel in one image are changed ,then the two images still look identical to human eye. This is because the human eye is not sensitive enough to notice the difference in color between pixels that are different from one unit.Thus steganography applications use LSB because attacker's do not notice anything odd or suspicious about an image if its LSB's are modified.

Unfortunately for every computer security strategy ,there are attackers who develop countermeasures to defeat that security strategy. Attackers combat steganography using steganalysis. Steganalysis is a process of where attackers analyze an image to determine whether it has hidden message .A common steganalysis approach is to graph the pixel value of image, statistical analysis is then performed to find anomalies. These anomalies may indicate that image contain hidden message.

In this paper a specific image based steganographic model has been proposed which uses a bit mapped image as a cover image and the secret information is stored in the cover image to form stego-image. Before storing the information is encrypted using RSA or Triple DES algorithm so that it can become more secure and than cipher text is stored using steganographic techniques .This paper also gives analysis of these algorithm in securing steganography based on factors like complexity ,changes, time and security.

Proposed Techniques:

This paper proposed two techniques, one is based on RSA algorithm and the other is based on Triple DES Algorithm. Both are explained below.

- *RSA based Technique:*

RSA is the most important public key encryption algorithm. It uses prime numbers to generate public and private key. It may be used to provide both secrecy and digital signature. It uses block size in which plaintext and cipher text are integers between 0 and n-1 for some n values .Size of n is considered 1024 bits or 309 decimal digits.Following steps are involved in this algorithm.

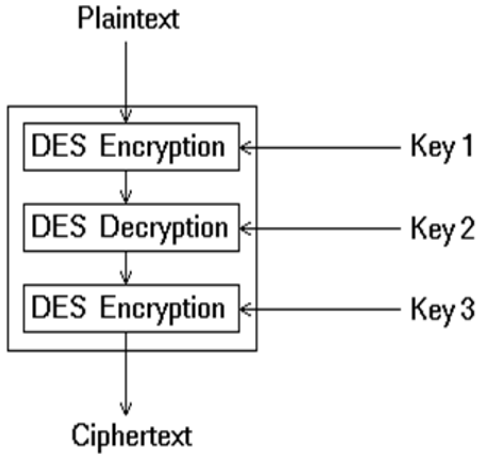
1. Select p, q, two prime numbers (private, chosen)
2. Calculate n = pq (public, calculated)
3. Calculate phi(n)=(p-1)(q-1)
4. Select e, with gcd(phi(n), e) = 1; 1 < e < f(n) (public, chosen)
5. Calculate $d = e^{-1} \pmod{phi(n)}$
6. Public key(e,n)
7. Private Key(d,n)
8. Encryption:Calculate cipher text ,$c=m^e \bmod(n)$
9. Decryption:Calculate Plaintext $m=c^d \bmod(n)$

In the proposed technique at the sender side, the information is first encrypted using RSA algorithm and then embedded in the cover image to obtain stego image. At the receiver side the stego image is taken and embedded information is extracted using steganographic technique and than decrypted using RSA method. Advantage of this algorithm is that there is no need to transfer key securely only public elements are shared.

- *Triple DES technique:*

Triple DES algorithm uses DES three times using three different key. Triple DES is

simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence,the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. This is shown in figure 3,



DES requires 16 rounds to encrypt the data block of 64 bit. The key used is of 56 bit. Sixteen permuted 48 bit key will be used in each round. Consequently, Triple DES runs three times slower than standard DES, but is much more secure. In single round of DES, the 64 bit input is divided into 32left-32 right bit. The Right 32 bit is processed further ,first it is expanded to 48 bit by using expansion table than 48 bit is XOR with key of 48 bit. The output is fed into 8 S-boxes to produce 32 bit output which is permuted by P-box and than XOR with left 32 bit.

The major advantage of Triple DES over simple DES is that as the key size triples, the security also increases. Simple DES only uses 56 bit key that makes it prone to brute force attack whereas Triple DES make use of 168 bit key in total making brute force attack infeasible.

Results and Discussion:

The paper compares the two algorithms based on the following different criteria

1. Data size: The input size is taken in Kilobytes and execution time in millisecond

   Table1: Execution time of encryption of different packet size.

Input Size(KB)	3DES(in millisecond)	RSA(in millisecond)
45	50	55
55	44	46
96	76	89
560	171	169

The table shows that triple DES execution time is less than the execution time of RSA.

2. Security:
   RSA is a public key algorithm so it does not require the secure transmission of key where as triple Des is a secret key algorithm so it requires the secure transmission of keys. than Triple DES .

3. Complexity:
   Complexity of RSA algorithm:
   - Let k be the length of n in bits $K=[\log_2 n]+1$
   - Adding two k bits integer O(k)
   - Multiplication of two k bits O(k) x O(k)=$O(k^2)$
   - Reduction modulo n of a 2k bit integer $O(k^2)$
   - Modular multiplication of two k bit integer $O(k^2)$
   - Complexity of each step of Euclidian algorithm $O(k^2)$
   - No. of iterations in Euclidian algorithm O(k)
   - Complexity of calculating d= $O(k^3)$

- Overall complexity of RSA is $O(k^3)$

Complexity of Triple DES algorithm

- Triple Des algorithm uses its own input for calculation in each round, so the complexity is O(logn)

4. Changes in bits: For a given input **"attack in morning"** ,the no. of bits changed in the images by using the algorithms for encryption.

Image	RSA Algorithm (no. of bits changed)	3DES Algorithm (no. of bits changed)
Image1	43	14
Image2	53	20
Image3	57	30

Table 2: No. of bits changed in the real image after steganography.

Conclusion:

The above results and discussion shows that Triple DES can be used effectively for securing Steganography because it takes less time, less complex, more secure and the changes in the image bit is less. The only thing to be considered is the secure transfer of the keys.

References:

[1]William Stalling ,*Cryptography and Network Security*,fourth edition,Prentice Hall.
[2] Jayeeta Majumder ,Sweta Mangal, "An Overview of Image Steganography using LSB Technique", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
[3]Aman Kumar,Dr.Sudesh Jakhar , "Comparitive Analysis between DES and RSA Algorithm's,"International Journal of Advanced Research in computer science and software engineering ,volume 2,Issue 7, July 2012.