A Survey on Cryptography and Steganography

Niveditha R

M.Tech Scholar, Akshaya Institute of Technology, Tumkur, Karnataka, India

Abstract: ***Cryptography is an area, which is developed to provide security for the sender and receiver to transmit and receive confidential data through an insecure channel by a means of process called encryption / decryption. Cryptography ensures that the message should be sent without any alternation and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography symmetric and asymmetric steganography. Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. The main objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. This paper includes the detailed survey on the steganography techniques and encryption algorithm with their merits and demerits.***

Keywords: cryptography, steganography, encryption algorithm, steganographic techniques

1. Introduction

Data security was found many years before the beginning of wireless communication. Processing and transmission of multimedia content over insecure network posses several security problems .To provide security attributers to multimedia contents, one needs to protect communicated information from unauthorized users. Multimedia content needs to be secured from different type of attacks, for example, interruption, interception, modification and fabrication. Peak signal to noise ratio and efficiency are two parameter are taken into consideration in order for the data security and safety.

Steganography and cryptography are the two approaches that makes the communication secures cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography is basically scrambling of data for ensuring secrecy and/or authenticity of information. Cryptography enables us to transmit data across insecure networks so that it cannot be read by anyone expect the authorized recipient. Steganography is the art and science to hide data in a cover that it can be text, audio, image, video etc.

Steganography is different from cryptography. The main objective of cryptography is to secure communication by changing the data into a form so that it cannot be understand by an eavesdropper. Over global transmission channels, people send sensitive personal information, corporate documents and financial transaction. As a result, multimedia data security has become a serious and major issues in telemedicine, military, E-commerce, financial transaction and mobile phone applications. For secure transmission of multimedia data, information should be concealed from adversaries or attackers. In such scenarios, security, integrity, authority and confidentiality of digital data should be provided.

The performance of a steganography system can be measured using several properties. The most important property s the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determined the existence of a hidden message other associated measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects and robustness, which refers to how well the steganographic system resists the extraction of hidden data.

2. Different Cryptographical Algorithms

2.1 Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography, it is widely used today. Following are the various goals cryptography [1].

a) Confidentiality:
   Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
b) Authentication:
   The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.
c) Integrity:
   Only the authorized party is allowed to modify the transmitted information. No one is between the sender and receivers are allowed to alter the given message.
d) Non repudiation:
   Ensures that neither the sender nor the receiver of message should be able to deny the transmission.
e) Access Control:
   Only the authorized parties are able to access the given information.

2.2 Cryptographical Algorithms

Encryption algorithm can be classified in to two broad categories - Symmetric and Asymmetric key.

A) DES

DES is a block cipher. It encrypts data in blocks of size 64 bits each.64bit of plain text goes as the input to DES, which produces 64 bits of cipher text. The keys length is 56 bits [2]. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness. This was based on symmetric key

algorithm which means that the same key will be used for both encryption and decryption.

DES can operate in CBC (chain block coding), ECB (Electronics codebook) and CFB (Cipher feedback) modes. DES has 16 rounds which mean a total of 16 processing steps are being applied on the input plaintext to produce cipher text. First, 64 bit data is passed through the initial permutation phase and then 16 rounds of processing takes place and finally the last step of final permutation is carried out on the input plaintext which results in 64 bit cipher text.

The drawback of this algorithm is that it can be easily prone to brute force attack in which the hacker attempts to break the key by applying all possible combination. In DES there are only 2^{56} possible combinations which are quite easy to crack. So DES is not so secure [3].

B) Triple DES

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching [4]. TDES uses three rounds of DES encryption and has a key length of 168 bits (56*3).Either two or three 56bit key are used in the sequence encrypt-decrypt-encrypt (EDE). First option is to use three different keys for the encryption algorithm to generate cipher text on plaintext message t.

$$C_{(t)} = E_{k1}(D_{k2}(E_{k3}(t)))$$

Where $C_{(t)}$ is the cipher text of plaintext message t, E_{k1} is the encryption method using key k1; D_{k2} is the decryption method using key k3.Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES.

$$C_{(t)} = E_{k1}(D_{k2}(E_{k3}(t)))$$

TDES with three keys requires 2^168 possible combinations and that of two keys requires 2^112 possible combinations to be tried out for brute force attack is practically not possible. This provides TDES as a strongest encryption algorithm which gives its application in banking industry. The disadvantage of this algorithm is that it is too consuming [1].

C) Advanced Encryption Standard (AES)

AES Is a variable bit block cipher and uses variable key length of 128,192 and 256bits.If both the block length and key length are 128 bits. AES will perform a processing round. If the blocks and keys are of 192 bits, AES performs 13 processing rounds [5]. Each processing rounds involves four steps.

i) Substitute bytes – uses an S- box to perform a byte substitution of the block.
ii) Shift rows – a simple permutation.
iii) Mix column – a substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix.
iv) Add round key – the key for the processing round is XORed with the data. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices.

D) Blowfish

Blowfish is a 64 bits block cipher with variable length key from 32bit (4 byte) to 448 bits (56 bits)[6]. The algorithm has two parts key expansion and data encryption. The key expansion step converts 448 its key into 4168 bytes. A P array of size18 and four S –boxes whose size is 256 each of which are initialized to hexadecimal digital of π. XOR each entry in P array and S boxes with 32 bits of the keys[7]. There are total 16 rounds of data encryption. In each round a 32 bit sub key is XORed with leftmost 32 bits of plaintext and the result is then passed to the F functions of blowfish. This result becomes rightmost32 bits for the next round and the output of F functions XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for the next round and so on. The F function is the kernel and distinguishing feature of blowfish.

The key of the blowfish algorithm is 448 bits, so it requires 2^{448} combinations to examine all keys [8]. The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation. It is simple to implement since all operation carried out are XOR and addition. Speed of encryption and decryption are also known to be faster than other popular existing algorithms [7].

E) RC2

RC2 is a block cipher with 64-bits block cipher and a variable key size that range from 8 to 128 bits. RC2 is vulnerable to a related key attack using 234 chosen plaintext.

F) RC6

RC6 is block cipher derived from RC5. It was designed to meet the necessities of the advanced encryption standard competition. RC6 proper has a block size of 128 bits and supports key size of 128, 192 and 256 bits. Some references consider RC6 as advance encryption standard.

G) RSA

RSA is a most popular and proven asymmetric crypto graphy algorithm. RSA is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers. Disadvantages of RSA algorithm takes more time for computation process. RSA takes more memory than AES and DES. RSA algorithm produces low level of output bytes

3. Steganography and Steganographic Methods

Steganography literally means covered writing. The goal of Steganography is to embed secret data in to a cover image in such a way that it will not be able to detect that a secret data exists in the image. The Steganographic system essentially needs a cover media which has redundant bits i.e., bits which can be the media. The techniques is to replace these redundant bits of the media with that of the secret data to be embedded. However as this method modifies the statistical properties of the media, it leaves behind detectable traces.

A Steganographic system is characterized by three different parameter which is deeply interrelated viz., capacity security and robustness capacity refers to the amount of data which can be reliably stared in the media, security is the inability of an intruder to extract the hidden data from the media and

robustness is the amount of modification that the stego – media can taken without destroying the secret data. Since the 8 – bit letter a only requires eight bytes to hide it in the ninth byte of the three pixels can be used to begin hiding the character the hidden message.

A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more and therefore it is more detectable .Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. Changes in these pixels are then avoided because slight changes would cause noticeable variations in the area [9] and [10].

While LSB insertion is very easy to implement, it is also easily attacked. Slight modifications in the color palette and simple image manipulation will destroy the entire hidden message. Some examples of these simple image manipulations include image resizing and cropping [11] and [12].

A new steganography method to hide a secret message into grayed- valued cover image was proposed. For embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. In each block, a difference value is calculated from the values is replaced by a new value to embed the value of the secret message. This method produces a more imperceptible result than those obtained from simple least- significant bit substitution methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image.

4. Steganographic Method

Steganographic method is classified in two methods:

i. Steganography in spatial domain
ii. Steganography in frequency domain

i) Steganography in spatial domain

In this method, the least significant bit of the cover image is modified with the data bits of the secret image. This leads to negligible changes to the cover image. This concept of least significant bit substitution includes the embedding of the secret data at the bits which having minimum weighting so that it will not affect the value of original pixel. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A= 01000001

Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only half he bits in an image be changed.

ii) Steganography in Frequency Domain

The need for enhanced security, has led to the development of other algorithm. LSB technique has weak resistance to attacks. So to overcome this shortcoming, researchers found a better way for hiding information in areas of the mage that are less exposed to compression ,cropping and image processing. The transform domain technique makes use of the transform co-efficient to hide the data. The secret data is embedded by modifying the transform co-efficient of the image which makes this technique more robust to attacks like compression, filtering etc. The different techniques used are DCT and DWT.

a) Discrete Cosine Transform (DCT)

In this the cover image is transformed from spatial domain to frequency domain. Two dimension DCT transformations is used. After applying quantization and IDCT on DC co-efficient, the encrypted secret image is embedded. This method uses JPEG compression algorithm to convert 8X8 – pixel blocks in to 64 DCT [13] co-efficient are modified to embed the encrypted secret .Since the methods works on frequency domain, it produces no noticeable changes in the visual appearance of the image. The disadvantages of this system are that it works only on JPEG files. In DCT, Encrypted secret image is placed in the low and mid frequency co-efficient.

The DCT is calculated using equation (1)

F (u,v) =1/4 c(u)c(v)

$$\sum_{x=0}^{7} f(x,y) \sum_{y=0}^{7} \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{\pi(2y+1)v}{16}\right]$$

For u=0…7 and v=0…7

$$\text{Where } C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k=0 \\ 1 & \text{otherwise} \end{cases} \quad (1)$$

The image recreated by applying inverses DCT according to equation (2)

F(x, y) =1/4 c(u)c(v)

$$\sum_{u=0}^{7} f(u,v) \sum_{y=0}^{7} \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{\pi(2y+1)v}{16}\right]$$

For u=0…7 and v=0…7

$$\text{Where } C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k=0 \\ 1 & \text{otherwise} \end{cases} \quad (2)$$

On reversing the frequency domain stego-image back to the spatial domain image may cause underflow and overflow problems.

b) Discrete wavelet transforms (DWT)

Wavelet transform (WT) converts spatial domain information to the frequency domain information wavelet are used in the image steganographic model because the wavelet transform clearly partitions the high frequency and low –frequency information on a pixel by pixel basis. Many

practical tests propose to use the wavelet transform domain for steganography because of a number of advantages. The use of seek transform will mainly address the capacity and robustness of the information hiding system features. In wavelet, both frequency response and time response information are known exact reconstruction is possible because of up sampling and down sampling of image. Advantages of DWT over DCT as, firstly no need to divide the input coding into non overlapping 20 blocks, it has higher compression ratio avoid blocking artifacts secondly, allows good localization both in time and spatial frequency domain. Thirdly, transformation of the whole image introduces inherent scaling. Finally better identification of which data is relevant to human perception higher high compression ratio. Figure 1 Shows the decomposition of image using DWT.

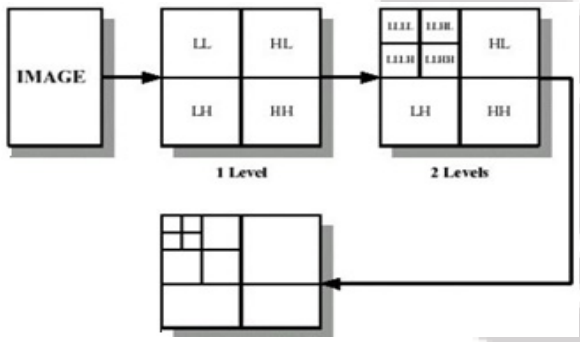

Figure 1

This method provides a high hiding capacity and good stego-image quality results analyses on the parameter peak signal to noise ratio by comparing the DCT domain and DWT domain. Peak signal to noise ratio is measure the quality of the stego-image by calculating the distortion between the stego-image and cover image higher the PSNR more is the security to image

5. Problem Description on Encryption Algorithm

Symmetric encryption users the same key concept to encrypt as well as decrypt, there are number of benefits of this approach. Performance is relatively high. There are two aspect of this algorithm. The first is the encryption algorithm and the other is the key the encryption algorithm is a process of transformation take place on the plain text with the key itself. At the time of decryption the same process of encryption is followed in a reverse manner with the same key. A strong algorithm should depends on its key entirely these algorithm can be directly implemented on hardware easily. The weakness of symmetric algorithm is in sharing of symmetric key between sender and receiver.

Asymmetric encryption users' two different keys for encryption and decryption. The private key can only decrypt the encrypted message. No key other than private key can be used for decryption the key exchange is not a problem in this approach. The public key can be known to anyone because it can be used only for encrypting the massage. So anyone can encrypt the massage but only the legitimate person can decrypt the message by using its own private key performance is relatively low as compared to symmetric key encryption. The problem asymmetric encryption is it works slower as compared to symmetric. Most asymmetric algorithm depends on the properties of hard problems in mathematics. These problems usually work intensive in one direction and nearly impossible in the other direction. For example, factoring the product of two large prime number. If one of the prime number is known the factoring becomes easy. but by knowing only the product it is very difficult to factorize and find the prime number.

6. Comparison of different Cryptographic Algorithms and Steganographic methods

Table 1: Throughput of DES AND 3DES, AES and BLOWFISH with different files size (MB/Sec)

Input size (Kb)	*DES*		*3DES*		*AES*		*BLOWFISH*	
	ENC	*DEC*	*ENC*	*DEC*	*ENC*	*DEC*	*ENC*	*DEC*
50	31	51	56	54	56	64	38	38
108	35	47	48	50	40	57	45	29
246	46	71	109	75	110	75	43	64
320	80	73	165	85	162	147	44	90
695	145	121	227	149	212	144	47	91
781	86	121	171	153	165	152	66	96
900	241	152	301	171	260	172	66	103
5500	248	166	307	178	258	170	118	100
7311	1692	952	1787	1100	1365	880	105	139
22300	1716	1196	1796	1700	1366	883	152	137
Average time	432	295.2	496.7	371.5	399.4	274.4	72.4	88.7
Throughput	8.64	12.65	7.52	10.05	9.35	13.61	51.59	42.11

Below fig 2 & 3 shows the throughput among different encryption and decryption algorithms.

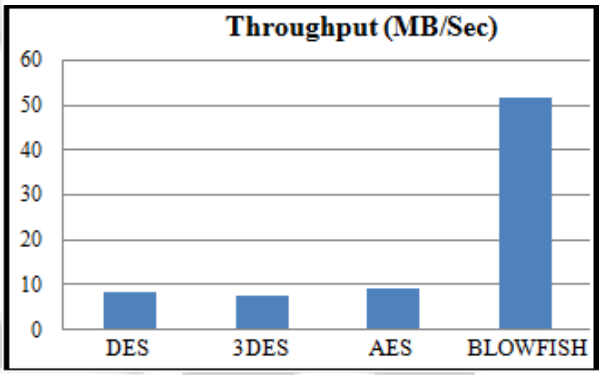

Figure 2: Throughput of encryption algorithm

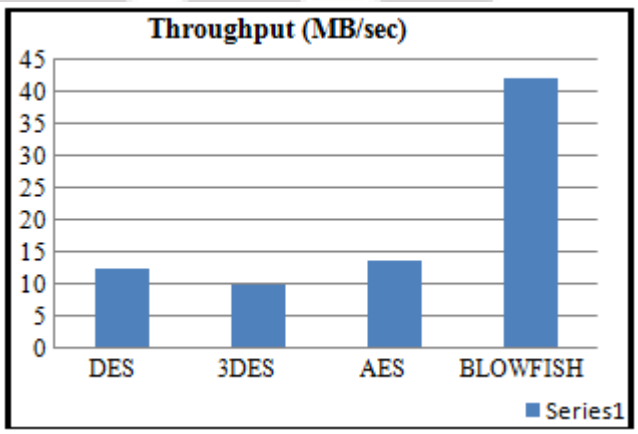

Figure 3: Throughput of decryption algorithm

Below fig 4 & 5 shows the power consumption among different encryption and decryption algorithms.

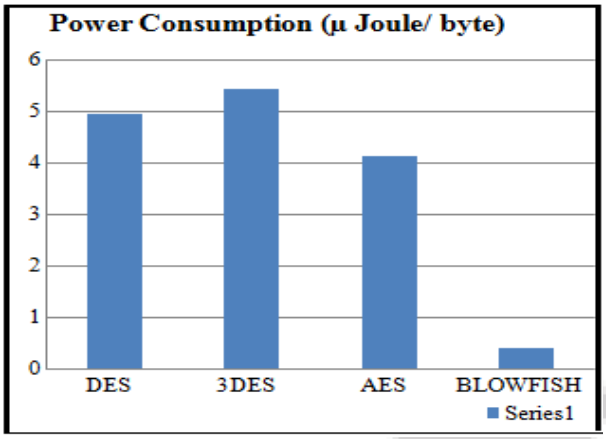

Figure 4: Power Consumption (µ Joule/ byte) of encryption algorithm

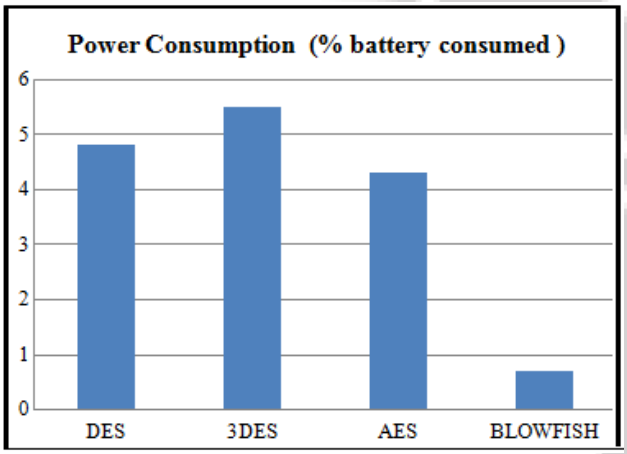

Figure 5: Power Consumption (µ Joule/ byte) of decryption algorithm

Table 2: Comparison between DWT And DCT On PSNR Value

Name of the image file	*Results obtain using spatial domain with RSA PSNR value (db)*	*Result obtain using DWT with RSA PSNR value (db)*
Barbara	51.165	78.13
Lenna	51.0728	78.01
Tulips	51.3453	78.00
Baboon	51.1490	72.33

7. Conclusion

This paper gives the survey on the image stegonographic techniques. Each technique satisfies the three important factors of data or secret message transmission. Under the spatial domain LSB techniques have a high payload capacity, but they often fail to prevent statically attacks and are thus easily detected. Similarly, under the transform domain techniques DCT and DWT play important role in transferring the image from spatial to frequency domain. The experiments have introduced some promising results and then they have diverted the researcher's attention toward JPEG image files. A DWT experimental result gives higher PSNR with DWT when compared with DCT and exact reconstruction is possible with DWT domain because of whole image encoded.

This paper also gives review of the popular symmetric key encryption algorithm such as DES, 3DES, AES and blowfish. Symmetric key algorithm runs faster than Asymmetric key algorithm such as RSA etc. The security aspect of symmetric key encryption is superior to asymmetric key encryption. The comparison of popular encryption algorithm clearly shows the blowfish algorithm gives the better throughputs, less power consumption and security over DES, 3DES and AES.

References

[1] O.P Verma, Ritu Agarwal ,Dhiraj Dofouti and Shobha Tyagi," Performance Analysis of Data Encryption Algorithms ",IEEE Delhi Technological University India ,2011.
[2] B. Suhnaier."Description of a New Variable Length Key.64 Bit Block Cipher (Blowfish) Fast Software encryption", Cambridge Security Workshop proceedings (Dec 1993), Springer-Verlang, 1994, pp.191-204.
[3] Diaa Salama, Abdul Minaam ,Hatem M .Abdual-Kader and Mohiy Mohamed Hadhond," Evaluating the effects of Symmetric Cryptography Algorithm an Power Consumption for Network Security.pp.78-87,Sep-2010.
[4] Aamer nadeem and Dr. M Yonus Javed," A Performance Comparison of Data Encryption Algorithm, IEEE 2005.
[5] Himani Agarwal and Monisha Sharma," Implementation and Analysis of Various Symmetric Cryptosystem, India Journal of Science and Technology Vol.3 No.12, Dec 2010.
[6] Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE 2009.
[7] Russell K. Meyers and Ahmed H. Desoky," An implementation of the Blowfish Cryptosystems", IEEE 2008.
[8] Michael C.J .Rin and Youn- Long Lin," A VLSI implementation of the Blowfish Encryption/Decryption Algorithm", IEEE 2000.
[9] Hiding Secrets in Computer files,"Steganography is the new invisible ink as codes away on images", –An article from: The futurist by Patrick fucker.
[10] Ismail Aveibas, Member ,IEEE, Nair Memon., Member, IEEE and Bulent Sankur, Member," Steganalysis Using Image Quality Metrics", IEEE Transcations on Image Processing , Vol 12.No.2.Feb 2003.
[11] Neils Provos and Peter Honeyman, University of Michigam,"Hide and Seek: An Introduction to Steganography,"IEEE Computer society IEEE Security & Privacy.
[12] R. Chandramouli and Nasir Memon," Analysis of LSB Based Image Steganography Techniques", 2001.
[13] K B Shiva Kumar." Bit Length Replacement Steganography Based on DCT Co-efficient", International Journal of Engineering Science and Technology, Vol.2 (8), pg: 3561-3570.2010.