Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancement Key of Cryptography and Stenography Using RSA

Prof. Ajit Singh
Dept. of CS & IT
BPS Mahila Vishwavidyalaya,
Khanpur Kalan, Sonepat,
Haryana, India

Preeti Kalra
M.tech (Network Security)
Dept. of CS & IT,
BPS Mahila Vishwavidyalaya,
Khanpur Kalan, Sonepat, Haryana, India

Abstract: - Cryptography and stenography are two processes used for sending information in secret way. Goal of both processes are to provide protection for information but in different way. In this paper our motive to represent a new method for protection that is generated by combination of both process stenography and cryptography. There are many algorithms exist for both processes. For cryptography there are algorithms like RSA, IDEA, AES, and DES but here we are using only one algorithm from these that is RSA which is enough to implement combined process. The encrypted image is used as input for neural network for further implementation. All implementation performed on the basis of the basis of PSNR, MSE parameters. So the image generated as result is encrypted that is very robust to attack.

Keyword: - Stenography, Cryptography, RSA, DES, key

I. INTRODUCTION

There are two processes exist that are used for sending information in secret way. These processes are known as cryptography [1] and stenography [1]. Both techniques widely used for protection of information or data. Stenography is art of that technique in which information hides on the way of communication between two nodes. Cryptography covert message in cipher text form so that it is not possible for unauthorized party to understand it. So the information hidden by stenography technique cannot see by any other person that is not authorized for it. In this paper we are going to develop a new system by using both processes stenography and cryptography. New system developed for better protection and confidently. Now days in market we have a cryptography technique - RSA very secure technique. After that we use custom neural network technique for applying second encryption technique to make more secure. Even we can apply these both techniques alone but any attacker can get original message by decrypt separately. So we apply both techniques at same time so any intruder cannot decrypt it or not as easy as single encryption technique can. This paper will highlight a new method that is developed for more security where image can be encrypted by using cryptography and stenography. We know how these processes can process as like:

- It is more secure if we send data in hidden form as compared to send it encrypted or visible to others.
- Main benefit of hidden data is that attention of intruder cannot notice.
- By chance if data extracted then it may be in encrypted form.

So there can any way to crack the encrypted image but the algorithm proposed by us has some well features with different way to implement as following:

- At place of hiding complete text in image we firstly segments according to 32*32 segmentation plan.
- To merge ascii encoded bits into the base image using public or private keys.
- Original message is accessible to that who knows about this with the help of keys that are used for encryption. Reverse process is applied to get original message.

Finally our object is to develop a method which is more secure and if anyone trying to access it from steno image [2] then it became waste for that intruder.

II. BASIC CONCEPT AND RELATED WORK

There are many techniques available for secure transmission through communication channel, one of these is cryptography. But it should be in mind that when only cryptography is applied for protection that is not sufficient to provide good security. There are some basic requirement for cryptography [3] as like integrity, redundancy, and authentication etc. there are basically three algorithms described for encryption as following: -

a) Symmetric cryptography: In this algorithm only a single key is used for encryption and decryption. The key used for cryptography is known as private key. key and encrypted data both are transmitted on different timing.
b) Asymmetric Cryptography: In this algorithm two keys are used for encryption and decryption. For encryption on sender side public key of receiver is used. On the receiving side means for decryption process private key of receiver is used.
c) Hash function: In this cryptography scheme mathematical concept is used for more protection.

As like cryptography, stenography is other technique that is used for secure communication. There are many ways to hide information like in audio, video [4], text, and any other digital representative. There are many techniques for data hiding like Substitution system, Transform domain techniques [5], Spread spectrum techniques, Statistical method, Distortion techniques [6], and Cover generation methods [6].

III. DES ALGORITHM FOR CRYPTOGRAPHY

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key.

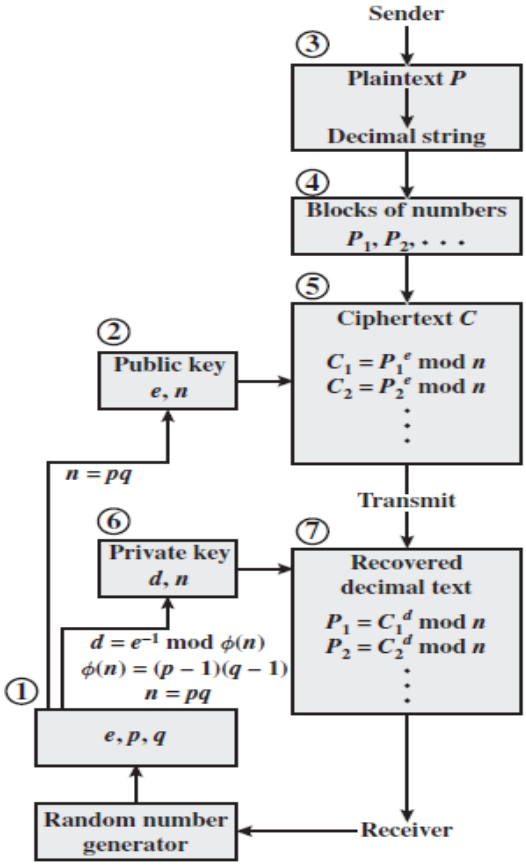

Fig 2: RSA processing of Multiple Blocks

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications.

The flow of DES Encryption algorithm is shown in Figure 3. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial

A. RSA ALGORITHM FOR CRYPTOGRAPHY

RSA based on a public key system that is generated by Ron **R**ivest, Adi**S**hamir, and Leonard **A**dleman in 1978 [9]. Three basic steps are required to complete the process of RSA operations that are; key generation, encryption and decryption. First, messages are converted to numbers (integers), and then the numbers are manipulated according to the prescribed encryption scheme. Here is the description of the RSA cryptosystem.For the implementation of RSA we have to follow following steps [10]:

Step 1 Firstly Choose two prime number p and q.
Step 2 Then compute value of n= p x q.
Step 3 Choose*e* with (e, (p − 1)(q − 1)) = 1 and computes *d* with $de \equiv 1 (\mathrm{mod}(p-1)(q-1))$.
Step 4 Makes n and e public and keeps p, q, and d secret.
Step 5 Sender encrypts *m* as $c \equiv m^e (\mathrm{mod} n)$ and sends *c* to Receiver
Step 6 Bob decrypts by computing $m \equiv c^d (\mathrm{mod} n)$.

B. NEURAL NETWORK IN CRYPTOGRAPHY

Neural networks are used in our proposed algorithm with RSA technique to get well encrypted image. In neural networks a node can be connected more than 40000 nodes for exchange information. The nodes in networks are called neurons. When a neuron is strongly connected to other neuron then both can exchange information. We are going to applying neural networks over the RSA technique. The way of computing in neural networks is shown in fig 1. As following:

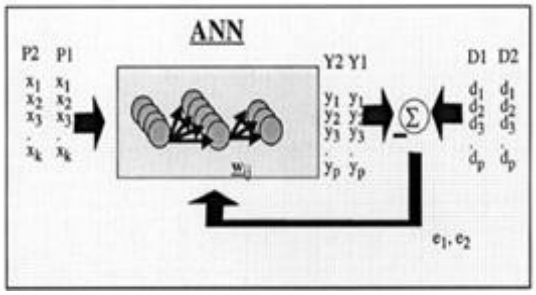

Fig 1 style of computing.

With the help of this algorithm decision taken on number of layers and number of nodes in hidden layers. When the connection in starting then assigned weight in randomly way.

There are two layer exist one is input and other is output. In input layer vectors that are pre-processed are presented and at output layer calculation of error performed. If error is finding at output layer then it comes on input layer by backward process. This process is continuing till the last pattern. This form one-iteration process. At end of every-iteration test patterns are presented to neural network, and the prediction performance of network is evaluated.

IV. COMPRISON OF EXISTING ALGORITHM

As the given figure represents the speed of RSA, Triple DESand DES algorithm to encrypt the data of same length.Throughput of the encryption algorithms is calculated bydividing the total plaintext in Megabytes encrypted on totalencryption time for each algorithm. Thus, if throughput increased than power consumption decreased. So, as speed ofthe DES encryption is twice times to the speed of RSAencryption speed.And DES alsoconsumes small power as comparison to RSA powerconsumption.

Table1: Execution Time (Milliseconds) of Encryption of Different data packet size

Input Size(KB)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	39	119
319	155	89	157
560	171	131	169
899	299	240	309
5345.28	1166	1296	1441
Throughput (MB/Sec.)	2.08	3.01	1.67

Table2: Execution Time (Milliseconds) of Decryption of Different data packet size

Input Size	3 DES	DES	RSA
45	49	34	61
55	47	22	59
96	63	53	57
236	67	62	64
319	85	98	154
560	161	125	163
899	171	152	183
5345.28	835	783	827
Throughput (MB/Sec.)	4.03	5.012	2.147

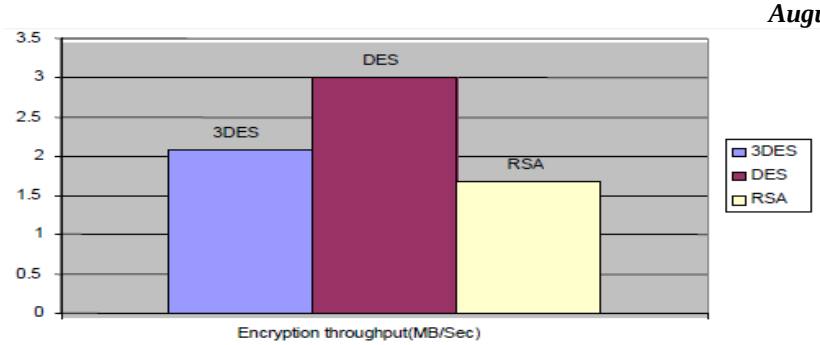

Fig.7 Decryption speed of RSA, 3DES and DES algorithms

Fig.6 Encryption speed of RSA, 3DES and DES algorithms

V. CONCLUSION

The selected algorithms DES and RSA are discussed withtheir working mechanisms. As DES is secret key basedalgorithm suffers from key distribution and key agreementproblems .But RSA consumes large amount of time toperform encryption and decryption operation Simulationresult showed that DES has better performance than RSA.From the simulation result, I evaluated that throughput ofDES algorithm is much better than the throughput of RSA algorithm. And, I also pragmatic that 3DES has more powerconsumption and less throughput than the DES due to itstriple phase characteristics. It had been also observed thatdecryption of DES algorithm is better than other algorithmsin throughput and less power consumption.

REFERANCES

[1] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134.

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

[3] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210.

[4] Chandramouli, R., Kharrazi, M. &Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[5] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[6] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996.

[7] N. F. Johnson and S. Katzenbeisser, .A survey of steganographictechniques., in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[8] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996

[9] Jung-Wen Lo, Min-Shiang Hwang, Chia-Hsin Liu, **"An Efficient Key Assignment Scheme for Access Control in a Large Leaf Class Hierarchy"** Information Sciences Vol. 181, 2011 pp. 917–925.

[10] C. Kaufman, R. Perlman, M. Speciner, **Network Security, Private Communication in a Public World**, Prentice Hall, 1995.

