



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

An Information Security Technique Using DES-RSA Hybrid and LSB

¹Sandeep Singh, ²Aman Singh

¹Department of Computer Science Engineering, Lovely Professional University,
Phagwara, Punjab, India

²Assistant Professor, Department of Computer Science Engineering, Lovely Professional University,
Phagwara, Punjab, India

Abstract: Security plays a vital role while exchanging large amount of information from source to destination. Currently technology is increasing very rapidly from security point of view. Each and every person wants his communication must be confidential and protected from the access of the illegal users over internet. Cryptography and Steganography plays a very important role as security tools. Cryptography is the art of converting the readable information into an unreadable form. Steganography is a tool used to hide information inside a media files such as images, audio and video etc. In this paper a combined technique of both cryptography and steganography is proposed for the better security of the data. The message is initially encrypted with DES and the keys of DES are encrypted with RSA then the hybrid of both DES-RSA is embedded inside an image with help of LSB image steganography. Results of the technique provide a stronger security. The encryption time is also faster than the previous techniques as well as brute force attack to this technique is almost not possible.

Keywords: DES; RSA; Hybridization; LSB; Steganography;

I. Introduction

The day by day development in the communication systems demands the very high level of information security in communication networks. As the transmission of information is increases on the internet so network security is getting very importance. Therefore the confidentiality and the reliability of the data must be protected from unauthorized access. It means there must be an explosive development in the field of information security along with the copyrights of the digital media. For the protection of secrete information cryptography and steganography are the two commonly used security tools. Confidentiality, accessibility and integrity are the three main concepts of information security. Opinions of the different people who make the use of such information are authentication, authorization and non-repudiation. Cryptography and Steganography are the security tools available for the protection of the secrete information.

Cryptography is an encryption technique used to convert the readable information into an unreadable form. It is of two type's symmetric and asymmetric key cryptography. In symmetric key cryptography same key is used for both encryption and decryption while in public key or asymmetric key cryptography different keys are used for both encryption and decryption i.e. public key for encryption and private key for decryption or vice versa.

Steganography Steganography is an information security tool which provides privacy of text or images to protect from disputer. Steganography insert the data in a cover image and changes its properties. Steganography generates secret messages so that hacker cannot notice the occurrence of message. So Steganography is the key of ability to avoid messages from exposure. Steganography is a Greek word , which means "covered writing." Steganography includes an immense collection of secret communications techniques which covers the message's persistence. The high-quality method of image Steganography aims at three aspects. First one is capacity, which means that maximum data can be stored within cover image, second one is the imperceptibility that describes the visual quality of stego-image after hiding the information and the last is robustness.

II. Various Encryption Algorithms

A. DES (Data Encryption Standard)

It was created in 1972 by IBM with the data encryption algorithm and was adopted by the US government as standard encryption technique for DES begins the encryption procedure by using a 64-bit key. DES wants two inputs - the plaintext to be encrypted and the secret key. The way in which the cleartext is received also the key agreement used for encryption and decryption, both confirm the type of cipher it is. DES is a symmetric key algorithm, 64 bit block cipher as it uses the similar key for both encryption and decryption and just operates on 64 bit blocks of information at a time 5 (be they plaintext or cipher text). The key size used is 56 bits, but a 64 bit (or eight-byte) key is actually input. The LSB of each byte is either used for equality (odd for DES) or set randomly and does not enlarge the security in any mode. All blocks are numbered from left to right which makes the eight bit of each one byte the parity bit.

Ever since its acceptance as a central standard there have been concerns about the level of security provided by DES in two areas, Key size and nature of the algorithm.

- 56 bit key length (approx 7.2×10^{16}) on early consideration brute-force attack seems unworkable. But with an extremely parallel machine of about 5000 nodes with every node able of achieving a key search rate of 50 million keys/sec, the time taken to perform a brute-force search is about 100 hrs which is far from extreme.
- The characteristic of DES algorithm: of additional concern is that cryptanalysis is achievable by exploiting the features of DES. The centre of attention is the eight S-boxes used in each iteration. The plan criteria for the whole algorithm has certainly not available and there has been rumour that the boxes were constructed in such a manner that cryptanalysis is achievable by a challenger who knows the weak points in the S-boxes.

B. RSA (Rivest, Shamir and Adleman)

It is the most important algorithm of the asymmetric key cryptography; it is able to resist all most all the possible attacks on the password till now. RSA represents the name of its inventors, first algorithm which provide both encryption as well as digital signature. Its security is lies on the mathematical computation of the two large prime numbers. In RSA two prime numbers are used for the creation of public key and private key. It is very difficult to know the original message from signal key. It is very much secured from brute force attack as well [6].

RSA algorithm can be basically described as Follows:

1. Generating keys of RSA
2. Choose two prime number p and q
 - a. $n = p \times q$
where n is a large integer whose factorization gives two large prime number p and q
3. $\phi(n) = (p - 1) \times (q - 1)$
4. Randomly select key encryption key
where $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$
5. Now solve the following equation to compute decryption key d
 $e \cdot d \equiv 1 \pmod{\phi(n)}$ and $0 \leq d < n$
6. public key $PU = e, n$
7. private key $PR = d, n$

C. Hybrid cryptography

Symmetric key algorithms are facing a problem related to the security of the keys and asymmetric key algorithms are facing the problem of very slow speed as compared to symmetric key algorithms. Symmetric key algorithms can be used for both large and small message transmission but asymmetric key algorithms are only well suitable for small message transformation over the internet. Therefore, to reduce or overcome from the problems of both symmetric and asymmetric key algorithms a hybrid of both these algorithms are used which is known as PGP (Pretty Good Privacy). It will provide the protection for the symmetric keys as well as increases the speed of the asymmetric key cryptography.

Advantages of hybrid cryptography:

- No need to send DES keys secretly before communication.
- Keys are sending by RSA, so it will also act as digital signature.
- Having same speed of encryption and decryption as DES.

D. LSB (Least significant bit)

It is a simple, efficient and easy to use technique that embeds data in a cover image [4]. For example, it would be an easy way to put the information at the least significant bit (LSB) of an image at every pixel. The embedded information will create a distorted image called stego-image. For a computer system, an image refers to a file that signifies some colours and that too with different intensities of brightness on different regions of that image. Usually steganography is the technique to hide data behind an object and that object may be any text, image, audio or video file. Various techniques are there in steganography to perform such hiding mechanism. One of those techniques is LSB. In the LSB technique, out of the total size of file, 8th bit of each byte gets replaced by one bit of the secret data. This technique is effective mostly in case of image files where substitution done creates least changes in the image so formed. The substitution done is performed from 0 to 1 or vice versa. The changes in the so formed image will be such that they cannot be significantly visible. The file created after LSB treatment hardly makes any change in the size of the data. But the output file may vary in its clarity or sometimes seems to be distorted.

LSB image steganography steps

1. According to key choose n hidden pixels from the image.

2. Determine k^{th} bit of information. ($0 < k \leq \text{length of data}$).
3. Now choose the k^{th} bit of hidden pixel and determine its pixel value. ($0 < k \leq m$).
4. If the LSB of the image pixel is same to information then left it unchanged otherwise proceed to next iteration.
5. Now replace the LSB of the image with the data bit and left the other 7 bits unchanged.
6. If all the information is embedded inside the image then end the method otherwise back to step 2 again.

III. Related Study

Sattar J Aboud, Mohammad A AL-Fayoumi, Mustafa Al-Fayoumi and Haidar S Jabbar (2008) purpose the enhanced version of RSA public key algorithm. It relies on the group of linear algebraic over ring of integers numbers which mod a composite modulus n that is the product of two prime numbers p and q . In this the original message and the encrypted message are in $h \times h$ matrices having parameters in Z_n denoted by $l(h, Z_n)$, where as in original RSA it is denoted by $(0, n-1)$ for modulus n . Brute force attack on RSA is almost very rear as it is based on mathematical factorization of prime numbers. RSA can be used for encryption and decryption as well as a digital signature scheme [8].

Sattar J Aboud purposed an algorithm to attack for RSA algorithm (2009). Main objective of the algorithm is to get the private key of RSA algorithm and then factoring the modulus based on the public key of RSA algorithm. Key generation algorithm was run 100 times to get the average key generation time that is only 93ms as compared to the RSA of small e method that is 42 seconds. For each loop the average numbers of iterations were 842 as compared to RSA small e method that is 37656. It not compute the complete prime factoring of p and q but it only tries to find the small factors until desired factoring. It is efficient key generation scheme. Decryption time is longer than a small e scheme RSA. Encryption is 2.6 times faster but decryption is 1.2 times slower. It is effective but having large number of iterations. It is more efficient algorithm for attack on RSA as it is faster and takes less time to run [7].

Tang Songsheng and Ma Xianzhen (2010) conducted the research on two block cipher algorithms (DES and AES). Weakness of the DES algorithm was shown on various aspects such as weak key and semi-weak keys, short key length and "Trap door". As there are 16 rounds in DES each of which use a different encryption sub-keys as an important feature for DES strength. Some of the keys generated overlap among themselves as the sub-key generation process is poorly designed, so the use of such weak keys can decrease DES security therefore these should be avoided in practical applications. DES keys are also short in length. Only 56 bit is valid and rest 8 bit is parity, so only 256 possible key combinations can be there for successful brute force attack. DES has only 8 S-boxes. The whole security of the algorithm lies in the non-linear component of the S-box, as its design standards are not announced yet, therefore it may hide the chances of successful attacks from an intruder [10].

Wuling Ren and Zhiqian Miao (2010) proposed hybrid encryption algorithm of DES-RSA to enhance the security of blue tooth communication. A hybrid encryption is used in blue tooth communication instead of E0 encryption. As E0 stream cipher is facing a problem that it cannot restore the plaintext from cipher text in decryption if pseudo-random sequence create an error, therefore it will affect the whole cipher text. The security of E0 relies on its internal mechanism of secrete key stream generator, if its output become endless zero then cipher text is a plain text, so it is a worthless. To overcome from all these hybrid encryption was introduced. In hybrid encryption the message is transmitted through DES and the keys are transmitted through RSA. Using together, so there will be no need to send the keys separately. Speed of encryption and decryption is same as that of DES. RSA can also be used as a digital signature. It is relatively more secure and easier to achieve than E0 [11].

Misbha Rum, Aihab Khan, Malik Sikander Hayat Khiyal (2011) Analysis of different pairs of encryption and decryption algorithms such as RSA-DES, RSA-AES and RSA-3DES is done as hybrid encryption techniques. It has been seen that the message passing between two different parties is secured by using hybrid approach. Conclusion was carried out on basis of execution time and memory uses. Table 2.1 shows results of the research shows that RSA-DES hybrid takes less time and consumes less memory as compared to others [5].

Table 2.1 Time and Memory Comparison of Hybrid Techniques

Message Size	RSA-AES		RSA-DES		RSA-3DES	
	Time Consumed	Memory Consumed	Time Consumed	Memory Consumed	Time Consumed	Memory Consumed
56 bits	273 ms	33114 kb	216 ms	32768 kb	287 ms	37683 kb
256 bits	307 ms	50467 kb	266 ms	37683 kb	290 ms	37723 kb
512 bits	311 ms	57344 kb	278 ms	37683 kb	309 ms	40960 kb

Monica Adriana Dagadita, Emil Ioan Slusanschi and Razvan Dobre (2013) proposed a least significant bits (LSB) approach using BMP images. Hiding a secrete message inside a image is most widely used and popular technique, as image is a most frequently used media in a internet, so no one can easily identify it. Serial and

parallel versions are proposed and performance is evaluated using images of size from 1.9 to 131 megapixels. Information hidden in an image depends on the size of the images and number of LSB used for encryption. It provides better efficiency and capacity. Quality of stego images is also good. PSNR ratio is also better than the existed techniques [12].

Zhiyi Fang, Ying Wang, Zelin Deng, Fan Yang (2013) proposed a secure key service mechanism in mobile network. The proposed technique was based on RSA-DES hybrid encryption technique. Analysis has been carried out among various algorithms such as DES, RSA and RSA-DES hybrid. It has been that response time of DES-RSA hybrid is fast than other two algorithms. Table 2.2 shows that DES-RSA provides more security than others also the scalability of the DES-RSA hybrid is very much stronger than the DES and RSA. Practicality of the DES-RSA hybrid is also stronger than the RSA and DES [13].

Table 2.2 Comparison between DES, RSA and DES-RSA

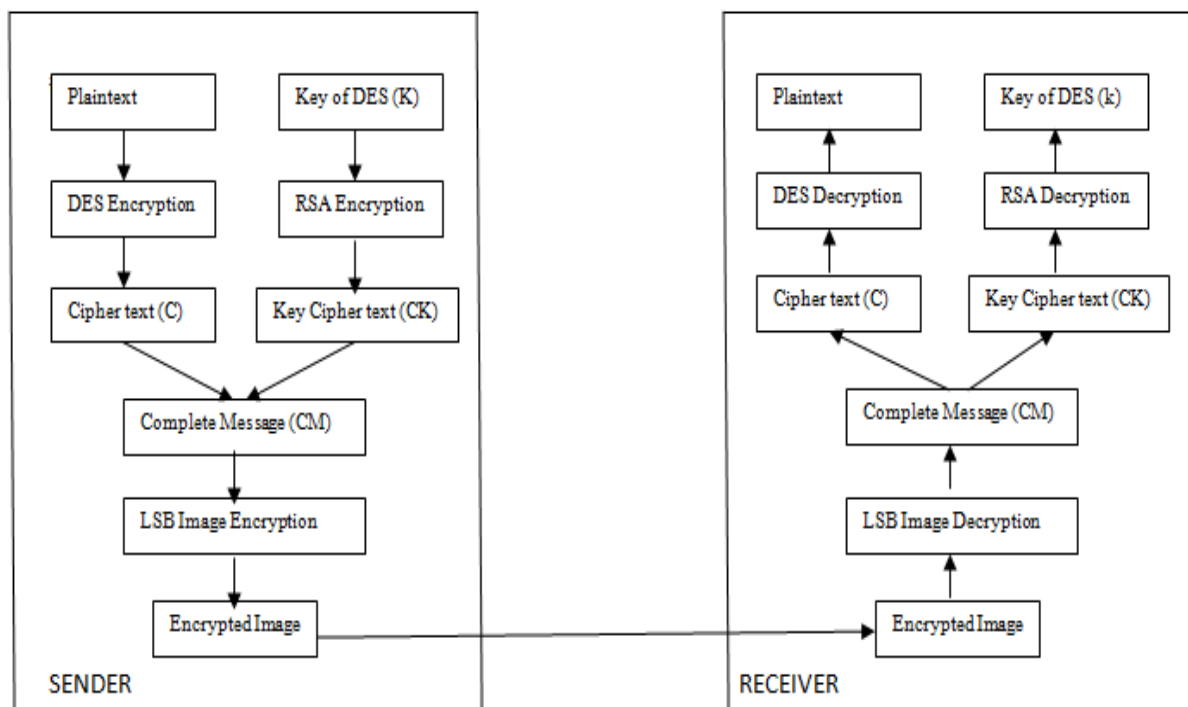
Factors	Algorithms→	DES	RSA	DES-RSA
Response time		Fast	Slower	Fast
Security		Weak	High	High
Scalability		Weak	Weak	Strong
Practicality		Weak	Weak	Strong

The proposed scheme is implemented in C# platform using standard cryptography and steganography algorithm. DES-RSA hybrid cryptography is used along with LSB image steganography.

IV. Proposed Methodology

The proposed scheme is implemented in C# platform using standard cryptography and steganography algorithm. DES-RSA hybrid cryptography is used along with LSB image steganography. Figure 1 shows the working of proposed information security scheme.

Figure 1 Proposed Information Security Scheme



For encoding steps are following:

Step 1: Encrypt the message with DES algorithm

Step 2: Choose any two prime numbers for the creation of RSA keys.

Step 3: Encrypt the DES keys with the public key of RSA generated from two prime numbers.

Step 4: Ciphertext of both DES and RSA is shuffled among themselves to represent a hybrid of ciphertexts.

Step 5: Hybrid of ciphertexts is hidden inside a image using LSB steganography.

Step 6: Stego image is generated for transmission.

For decoding steps are following:

Step 1: Stego image received from sender.

Step2: Obtain the hybrid ciphertexts from the stego image by decoding it using keys of LSB.
Step3: Extract the DES keys from the ciphertext of keys using private key of RSA.
Step4: Now use the keys obtained from RSA to decrypt the ciphertext of DES.
Step5: The real information is available now for the receiver.

V. Results and Discussions

Proposed model is stronger information security technique because without knowing the secret behind the hybrid of DES-RSA ciphertext no one can easily be able to identify that how to break it and generate two different ciphertexts from it. It has been seen that this scheme is far better than the previous scheme in which only DES and LSB is used. Brute force attack can be easily used on the ciphertext of DES to generate its keys but in proposed technique the brute attack is almost not possible until or unless the hybrid is not broken. So for the protection of DES keys RSA is used for it and a hybrid of both ciphertexts is generated. Same plaintext and same key is given to both proposed and previous techniques. It has been clearly seen that to break the ciphertext of DES is far easier than to break hybrid ciphertexts.

Figure 2 Ciphertext of DES

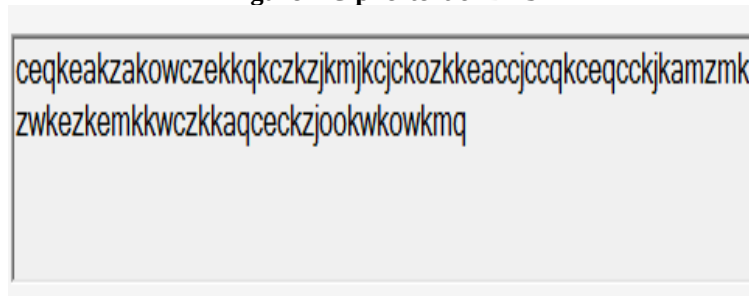


Fig 3 Ciphertext of RSA

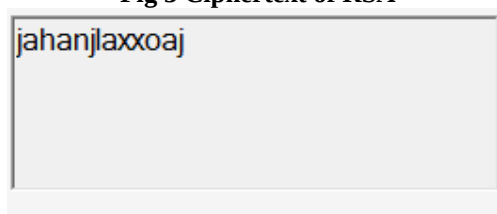


Fig 4 Ciphertext of DES-RSA Hybrid

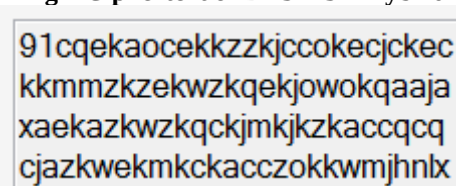


Figure 2 shows the ciphertext of DES, it can be very easily cracked by brute force attack by keep trying all possible key combinations. Figure 3 shows the ciphertext of RSA which encrypts the keys of DES so for the keys of DES RSA should be cracked first but it is not easy as it is looking. Figure 4 shows the hybrid ciphertext of both DES and RSA. It provides a very strong security to the system. No one can crack the system until or unless the two ciphertexts are not separated from the hybrid. No doubt that it will never be broken, it can be cracked but it takes a very long time than a simple DES. So it is clear from Figure 4 that it is very difficult to crack the hybrid therefore it provides a stronger security than the existed technique.

Timing evaluation of the proposed technique is also better than the previous technique.

Plaintext → Lovely Professional University

Key → Jalandharroad

Figure 5 Encryption time of proposed technique

Algorithm	Time in ms
DES	4ms
RSA	752ms
DES-RSA	50ms
Total Time	273ms

Figure 6 Encryption time of previous technique

Algorithm	Time in ms
DES	5ms
Total Time	412ms

From figure 5 and figure 6 is clear that the encryption time taken by the proposed technique is better than the previous technique.

VI. Conclusion

In the proposed method the strength of DES-RSA hybrid increase the level of security as compared to the existing technique where only DES is used. In this method the message is encrypted with a DES and the keys of DES are again encrypted with a RSA then the hybrid of both ciphertext is hidden inside an image using LSB image steganography. Steganography, specially shared with the cryptography is a stronger tool which allows exchanging information secretly. With the fast growth of digital technology and internet, steganography has highly developed a lot in a past few years. It will test the knowledge of the attacker about both cryptography and steganography. If an attacker is able to extract data from image then he has to crack the hybrid cryptography then only he will get the exact data. A result of proposed technique shows that the encryption time is better than the existing technique. It provides a more security compared to the existing one. Brute force attack on this technique is very difficult to use as there is use of RSA for DES key. In future other steganography techniques may be used with hybrid cryptography for more security.

VII. References

- [1] Gutub A A, and Khan F. A. (2012) Hybrid crypto hardware utilizing symmetric-key & public-key cryptosystems, International Conference on Advanced Computer Science Applications and Technologies, page(s): 116-121.
- [2] Harshali D Z and Prakash W W. (2012) Design and Implementation of Algorithm for DES Cryptanalysis, Hybrid Intelligent Systems (HIS), 2012 12th International Conference on 4-7 December 2012, page(s): 278-282.
- [3] Hybrid Cryptography for Improving Data embedding Capacity, Communication, Information & Computing Technology (ICCICT), 2012 International Conference on 19-20 October 2012, page(s): 1-6.
- [4] Monica A D, Emil I S and Razvan D. (2013) Data Hiding Using Steganography, Parallel and Distributed Computing (ISPD), 2013 IEEE 12th International Symposium on 27-30 June 2013, page(s):159-166.
- [5] Misbha I, Aihab K and Malik S H K. (2011) Confidentiality of Messages in a Cardless Electronic Payment System, Publication of Little Lion Scientific R & D, Islamabad Pakistan, page(s): 29-32.
- [6] Ramaiya M K, Hemrajani N and Saxena A K (2013) Improvisation of security aspect in steganography applying DES,” Communication systems and network technologies (CSNT), International conference, page(s):431-436.
- [7] Sattar J. (2009) An Efficient Method for Attack RSA Scheme, Applications of Digital Information and Web Technologies, 2009. ICADIWT '09. Second International Conference on the 4-6 August 2009, page(s): 587-591.
- [8] Sattar J, Mohammad A, Mustafa Al and Haidar S. (2008) An Efficient RSA Public Key Encryption Scheme, Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on 7-9 April 2008, page(s): 127-130.
- [9] Shand M and Vuillemin J. (1993) Fast Implementations of RSA Cryptography, Computer Arithmetic, 1993. Proceedings. 11th Symposium on 29 June- 2 July 1993, page(s): 252-259.
- [10] Tang S and Ma X. (2010) Research of Typical Block Cipher Algorithms, Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on 24-26 August 2010, page(s): 319-321.
- [11] Wuling R and Zhiqian M. (2010) A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication, Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on 15-16 May 2010, page(s): 221-225.
- [12] Yongzhen Z, Fenlin L, Xiangyang L and Chunfang Y. (2102) A Method Based on Feature Matching to Identify Steganography Software, Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on 2-4 November 2012, page(s): 989-994.
- [13] Zhiyi F, Ying W, Zelin D and Fan Y. (2013) The Research on NSSC Key Service Mechanism in Mobile Network, 2nd International Conference on Science and Social Research (ICSSR 2013).