ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

Implementation of Image Encryption Algorithms to Camera Images

Shikha Roy, Sugandha Agarwal, Anil Kumar

Student, Dept. of Electronics and Communication, Amity University, India

Assistant Professor, Dept. of Electronics and Communication, Amity University, India

Head of Institution, Dept. of Electronics and Communication, Amity University, India

ABSTRACT: Information Security is of utmost significance parameter in the field of network communication system and Internet. To attain high level of security, integrity and confidentiality, image encryption algorithms have been utilized, as it provides a reliable, secure and efficient way to communicate the information to the assigned users, without the interruption of brute force attacks. This paper aims in presenting a comparison of performance of image encryption algorithms, namely, Data Encryption Standard (DES) and Rivest Shamir Adlemen (RSA) in terms of data security, confidentiality, integrity, and authenticity of the images. Analysis of result shows that RSA based encryption algorithm gives a good results in terms of high security and tunability.

KEYWORDS: Image Encryption, DES, RSA

I. INTRODUCTION

The concept of image encryption algorithm in data communication network is to send secure and reliable information to the intended users, without introducing inconsistencies or artifacts, during transmission, otherwise, which may tamper the attribute of the actual information. Encryption is the process of transforming the information for its security. With the enormous development of internet networks and the newest advances in digital technologies, it is of utmost requirement to send the secure information over various types of networks. Further, it is enormously important and indispensable for user performing e-transactions. To accomplish this task, a number of image encryption schemes have been developed to fulfill the demand of secure transmission of information over the Internet and wireless networks. Moreover, substantial research on the development of image encryption algorithms has been carried out at regular intervals to overcome the limitations associated with the encryption algorithms.

Furthermore, a large number of studies have been carried to highlight the utility and significance of image encryption algorithms [1]. These encryption algorithms are responsible for providing security, confidentiality, non-repudiation, integrity and authenticity of secret data. This can be classified into Symmetric and Asymmetric keys encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt data, whereas, in Asymmetric key, there is a provision of two keys one is public key, used for encryption and other is private key, used for decryption [1-3].

Encryption algorithm consists of Plain text and Cipher text. The former provides the original data which the sender intends to send, while the latter provides the encrypted format of the plain text. In other words, the plain text is converted to the Cipher text and vice versa with the help of an encryption and decryption algorithm. Some of the well known and commonly used encryption algorithms are DES and RSA. DES encryption algorithms is based on the concept of the secret key, and suffers with problem of key distribution and key agreement problems. In order to resolve this problem, a concept of asymmetric algorithm has been introduced by [14]. The asymmetric algorithm is based on the concept of 'Private Key and Public Key'. These keys are used for encryption and decryption.

Thus, the main objective of this study is to investigate and analyze the existing encryption algorithms, such as DES and RSA in terms of security, key size, Block size, authenticity of secret data and encryption and decryption time.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

II. IMAGE ENCRYPTION ALGORITHMS

Image encryption algorithms are brodly classified as Symmetric Key Algorithm (SKA) and Asymmetric Key Algorithm (AKA). Algorithm such as, Data Encryption Standard (DES) belongs to SKA, whereas, algorithm such as, Rivest Shamir Adlemen (RSA), belongs to AKA. In symmetric key algorithm, single key is used for encryption and decryption. Therefore, on receiving the message, it is impossible to decrypt it unless the key is known to the recipient. To transmit information securely, the keys should be known to sender and recipient only. If the key for transmission is leaked out, then the information can be stolen by the intruder.

In this study, a well known Symmetric algorithm such as, Data Encryption Standard (DES) have been selected for analysis [1-4]. Asymmetric key cryptography, also known as public key cryptography, developed by Whitfield Diffie and Martin Hellman. In public key cryptography, keys used for encryption and decryption are different. It is very important to note that even with the knowledge of the cryptographic algorithm and the encryption key, it is computationally infeasible to determine the decryption key [13-14]. The advantage of this system is that each communicating party requires just a key pair for communicating with any number of other communicating parties. Further, a well known AKA is RSA, offers an important characteristic for providing two related keys i.e., 'Private Key and Public Key'. These keys are used for encryption and decryption. In other words, the the plain text can be encrypted by sender with help of public key and the cipher text can be decrypted with the help of its private key [15-16].

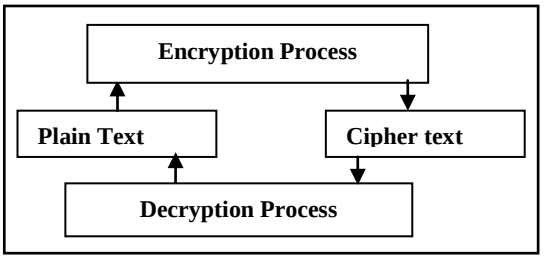

Figure 1: Encryption and Decryption process

2.1.1 Data Encryption Standard (DES) Algorithm

One of the most well known encryption scheme widely used for over two decades is known as the Data Encryption Standard (DES), is a symmetric key block cipher algorithm which was developed by IBM in 1977. DES algorithm uses the same key of size of 56-bits and block size of 64-bits, for encryption and decryption. It consists of a fiestal network which divides a block into two equal Halves where the right half passes through a function. DES has series of S boxes and P-boxes [5-7]. After passing through the Initial Permutation (IP) and substitution box the cipher text is obtained by the Ex-or operation which takes place within the set of rounds [8-9]. Decryption is just the reverse process. The encryption procedure of images using DES algorithm [3-6].can be summarized as follows:

1) Plain text of length 64 bit has taken, along with key of 56 bit to generate output of 64 bit block. Thereafter, plaintext executes the encryption function IP to generate the performs an Initial Permutation (IP), followed by a reverse final permutation.
2) Plain text of 64 bit passes through an IP that rearranges the bit to generate the permutated bit, which in turn produces left plain text and right plain text.
3) Encryption process is carried out for 16 times with its own keys.
4) The output of above encryption process comprises of 64 bits obtained from plain text and key.
5) Finally, the output is subjected to inverse IP to produce 64 bit cipher text.

Since DES is vulnerable to brute force attacks therefore it is proven inadequate in terms of security. In order to overcome this weakness, asymmetric algorithm, known as, Rivest Shamir Adlemen encryption algorithm was introduced.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

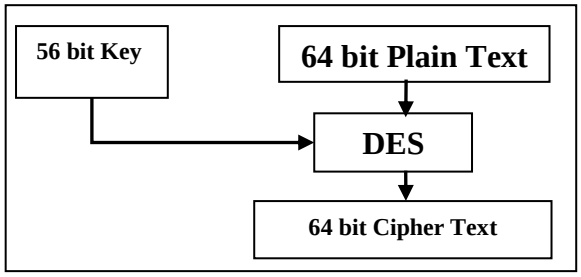

Figure 2: DES Process

2.2.1 Rivest Shamir Adlemen (RSA)

It is one of the most popular public key encryption algorithm concluded the problem of key distribution has by Asymmetric key encryption, in which two keys are used; public K_E and private K_D keys, as shown in Figure 3. It offers good security and secured digital signature. It uses the co-prime numbers to generate the public K_E and private K_D keys. Here, the encryption key used is known to sender and decryption key is to receiver [4]. The data used in this are block size data in which plaintext and cipher text are integers ranges between 0 and n.

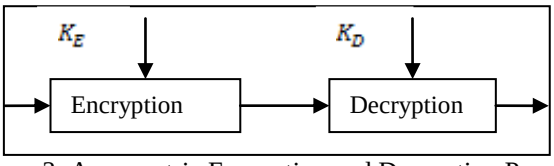

Figure 3: Asymmetric Encryption and Decryption Process

Further, the security of RSA relies upon the complexity of factoring integers into their prime factors. It offers reliable and secure transmission of data [16]. There are many applications for RSA ranges from banking, e-mail. Digital signatures, digital certificates on the Internet and encryption of small pieces of data and for key transport [14-18]. Furthermore, RSA can be used for application in wireless network, as it offers reliable security and enhanced speed.

The encryption procedure of images using RSA can be summarized as follows:

1) Select two distinctive primes p and q and then form the public modulus $n = RS$.

2) Select public exponent e to be co-prime to $(R-1)(S-1)$,with $1 < e < (R-1)(S-1)$.

3) The pair (n, e) is the public key.

4) The private key is the exclusive integer $1 < d < (R-1)(S-1)$ such that $ed = 1 \bmod (R-1)(S-1)$.

Encryption: Message M is split into a sequence of blocks $M_1, M_2, \ldots, M_t$ where each M_i satisfies $0 \leq M_i < n$. Then encrypt these blocks as

$$C \equiv E(M) \equiv M^e (mod\ n) \quad \ldots(1)$$

Decryption: Given the private key d and the cipher text C, the decryption function is:

$$D(C) \equiv C^d (mod\ n) \quad \ldots(2)$$

Although RSA is a secure algorithm, still there is a problem of weak keys. In order to resolve this shortcoming, digital signature concept was introduced in combination with RSA [17-18], which provides high security of the algorithm. This encryption algorithm found applications in electronic commerce trade, confidentiality, authentication, non-repudiation and construction of mercurial commitments.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

III. COMPARATIVE ANALYSIS

Table 1 shows the comparative analysis between symmetric and asymmetric algorithm in terms of different parameters, such as key length, block size, security and tunability. Comparing with the RSA algorithm, DES is the most insecure algorithm as it has already been declared inadequate to use. Further, it is also found that DES algorithm is vulnerable to brute force attacks, whereas in case of RSA intrusion is difficult.

3.1 Analysis based on Key Size, Block size and Security

Here, in this study, more emphasis has been given to security, as it plays a significant role in dtata communication network, internet and banking sector. The results of various attributes for diffrent image encryption algorithms are tabulated in Table 1.

Table 1: Comparative analysis of different encryption algorithms in terms of different attributes

Factors	***DES***	***RSA***
Key Size	*56 bits*	*>1024 bits*
Block Size	*64 bits*	*Minimum 512 bits*
Algorithm	*Symmetric*	*Asymmetric*
Tunability	*No*	*Yes*
Security	*Not Secure Enough*	*Secure*
Key Used	*Same key used for Encryption and Decryption*	*Different key used for Encryption and Decryption*

Further, it has been observed that RSA yields good results in terms of security, when compared to DES based encryption algorithm. In other words, the Asymmetric RSA algorithm gives good results in terms of security and tunability. Thus, it has been inferred that depending upon the type of applications, the encryption algorithm could be used.

3.2 Analysis based on Encryption and Decryption Time for different packet Size

Encryption and Decryption time also plays an important role while evaluating the performance of image encryption algorithms.

Table 2: Encryption and Decryption time involved for different encryption algorithms

Algorithm	***Packet Size KB)***	***Encryption Time (Sec)***	***Decryption Time (Sec)***
DES	*153*	*2.9*	*1.2*
RSA		*5.3*	*4.9*
DES	*196*	*2.0*	*1.3*
RSA		*6.5*	*5.9*
DES	*312*	*3.0*	*1.3*
RSA		*6.8*	*5.1*

Further, it is a function of encryption algorithm, image dimensions, software used and hardware specifications. The results of different fusion techniques in terms of computation time are given in Table 2.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

IV. CONCLUSION

In this study, a comparative study of DES and RSA encryption algorithm has been carried out in terms of key size, block size, tunability, security, and encryption and decryption time. Analysis of result shows that amongst the encryption algorithms, RSA is one of the most effective encryption algorithm in terms of security and tunability.

Eventually, it is concluded from this study that the image encryption algorithms is indispensable for secure and reliable transmission of data over the networks. Further, the choice of encryption algorithm is application dependent.

REFERENCES

1. Aman Kumar, Dr.Sudesh Jakhar, Mr. Sunil Maakar "Distinction between Secret key and Public key Cryptography with existing Glitches" IJEIM0067, vol.1, 2012
2. J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, ISBN: 978-0-387-77993-5, 2008.
3. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall, 2005.
4. Ruangchaijatupon, P. Krishnamurthy, „"Encryption and Power Consumption in Wireless LANs-N, "The Third IEEE Workshop on Wireless LANs-Newton, Massachusetts, 2001
5. T. Bala and Y. Kumar, "Asymmetric Algorithms and Symmetric Algorithms: A Review," International Journal of Computer Applications (ICAET), pp. 1-4, 2015.
6. M. Ebrahim, S.Khan and U.B.Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, vol. 61, pp. 12-19, 2013.
7. Singhand and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, " IEEE International Journal of Computer Applications, ,vol.67,pp.33-38, 2013.
8. W. Y. Zibideh and M. M. Matalgah , "Modified-DES Encryption Algorithm with Improved BER Performance in Wireless Communication," IEEE Radio and Wireless Symposium (RWS) Phoenix, pp. 219-222 , 2011.
9. S. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using Steganography, AES and RSA," IEEE Design and Technology in Electronic Packaging (SIITME) Timisoara, pp.339344, October 2011.
10. R.Rivest, A.Shamir, and L.Adleman, "A Method For Obtaining Digital Signatures and Public Key Cryptosystems," ACM Transactions on Communications, vol. 21, pp. 120-126, 1978.
11. M. Wang and Y. Que, "The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm," IEEE Computer Science-Technology App. IFCSTA Chongqing, vol. 2, pp. 24-28, 2009.
12. A. Mousa, "Data Encryption Performance Based on Blowfish," IEEE ELMAR Symposium Zadar, pp. 131- 134, 2005.
13. C, Michael, The RSA Cryptosystem: History, Algorithm, Primes, 2007
14. Ying-yu Cao, Chong Fu, "An Efficient Implementation of RSA Digital Signature Algorithm," IEEE Wireless Communications Networking and Mobile Computing (WiCOM) Dalian, pp.1-4, 2008.
15. LIU Dong-liang, CHEN Yan-ping, Z. Huai-ping, "Secure Applications of RSA System in the Electronic Commerce," IEEE Future Information Technology and Management Engineering (FITME) Changzhou, vol. 1, pp.86-89, 2009.
16. U. Somani , K. Lakhani , M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," IEEE Parallel Distributed and Grid Computing (PDGC) Solan , pp.211-216, 2010.
17. Hongwei Si, Youlin Cai, Zhimei Cheng, "An Improved RSA Signature Algorithm based on Complex Numeric Operation Function," IEEE Challenges in Environmental Science and Computer Engineering (CESCE) China, vol.2, pp. 397-400, 2010.
18. V. Mahalle, A.K Shahade , "Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm," IEEE Power, Automation and Communication (INPAC) Amravati, pp. 146-149, 2014.