ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available online at: https://www.ijergs.in

Volume - 5, Issue - 5, September - October - 2019, Page No. 09 - 14

An Overview of Image Encryption Techniques

[1]Khushboo Joshi, [2]Mr. Dheeraj Shrivastava

[1]M.Tech Student, Department of ECE, AIET, Jaipur (Raj), India

[2]Associate Professor, Department of ECE, AIET, Jaipur (Raj), India

Email : khushboostylejoshi@gmail.com, erdhirajshrivastava@gmail.com

Abstract

Today, the world is going to be digitized anyway. Each business unit, each government and private sector, each research unit uses the digital image as a transfer mode for all critical data. These images on the internet will not be secure. Therefore, there is a need for image security. Due to the rapid growth of digital communication and multimedia application, security becomes important issue of communication and storage of images. Encryption is one of the ways to ensure high security. The images are used in many fields, such as medical, military science. Modern cryptography provides techniques to protect information and protect multimedia data. In recent years, encryption technology has it developed rapidly and many image encryption methods were used to protect the confidential image data Unauthorized access. In this paper, different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used and also discusses the basic image security techniques, the survey of the recent research in the field of image securities.

Keywords : Cryptography, Decryption, Encryption, Image Encryption, Symmetric Key, Asymmetric Key.

1. Introduction

In today's world, security is an important factor for data storage and transfer in public networks. We can use cryptography to protect our files and communications. Cryptography is the art and science of encrypting data so that no one, except the sender and the receiver, realizes the original data, a form of security in the dark. Image is one of the most important information representation styles and is widely used in many applications such as military communication, telemedicine, medical images, etc. Images are often exchanged between two parties via unsecured networks. The image of the communication mode used in the different regions, the median, the research area, the negotiation zone, the military zone, etc. The transfer of important images is to make a trip from an unsecured Internet network. From that moment, it is necessary to choose a security service so that we can imagine that the person does not have access to important information. The wind effect of the image cubes that more multimedia data and protection needs. Cryptography is a tool for methodizing the image; It offers the secure method of transmission and purchase for the image of travel over the Internet. Security is the main concern of any system to maintain the integrity, confidentiality and authenticity of the image. At least cryptography is the elective method, but also the issue of proportional severity and gray-scale data is more [3].

2. Image Encryption

Encryption is the study of techniques to guarantee the communication process between the sender and the receiver in the presence of third parties called "liabilities". Essentially, it is understood that the design of protocols based on

mathematics, computer science and electrical engineering encrypt and decipher information in the form of data and images.

becomes even more important. To ensure such security and privacy for the user, it is very important to encrypt the image to protect against unauthorized access. Encryption of pictures and video is employed in varied fields, as well as web communications, multimedia system systems, medical imaging, telemedicine and military communications. color pictures ar transmitted and keep in massive quantities via the net and wireless networks that use the speedy development of multimedia system and network technologies. Cryptography has played an important role in security, and this is the battlefield for mathematicians and scientists from Shannon since 1949. Several cryptographic algorithms are now offered as AES, DES, RSA, IDEA, etc [6].

The image is the communication mode most used in different fields such as medical field, research field, industry, military area, etc. The important transfer of images will take place in an unsecured Internet network. Therefore, there is a need for appropriate security so that the image prevents access by the unauthorized.

Modern cryptography can be classified broadly into two types:-

A. Symmetric key cryptography

In the form of encryption, there is only one key and the private key is used to encrypt and decrypt data between the sender and receiver.

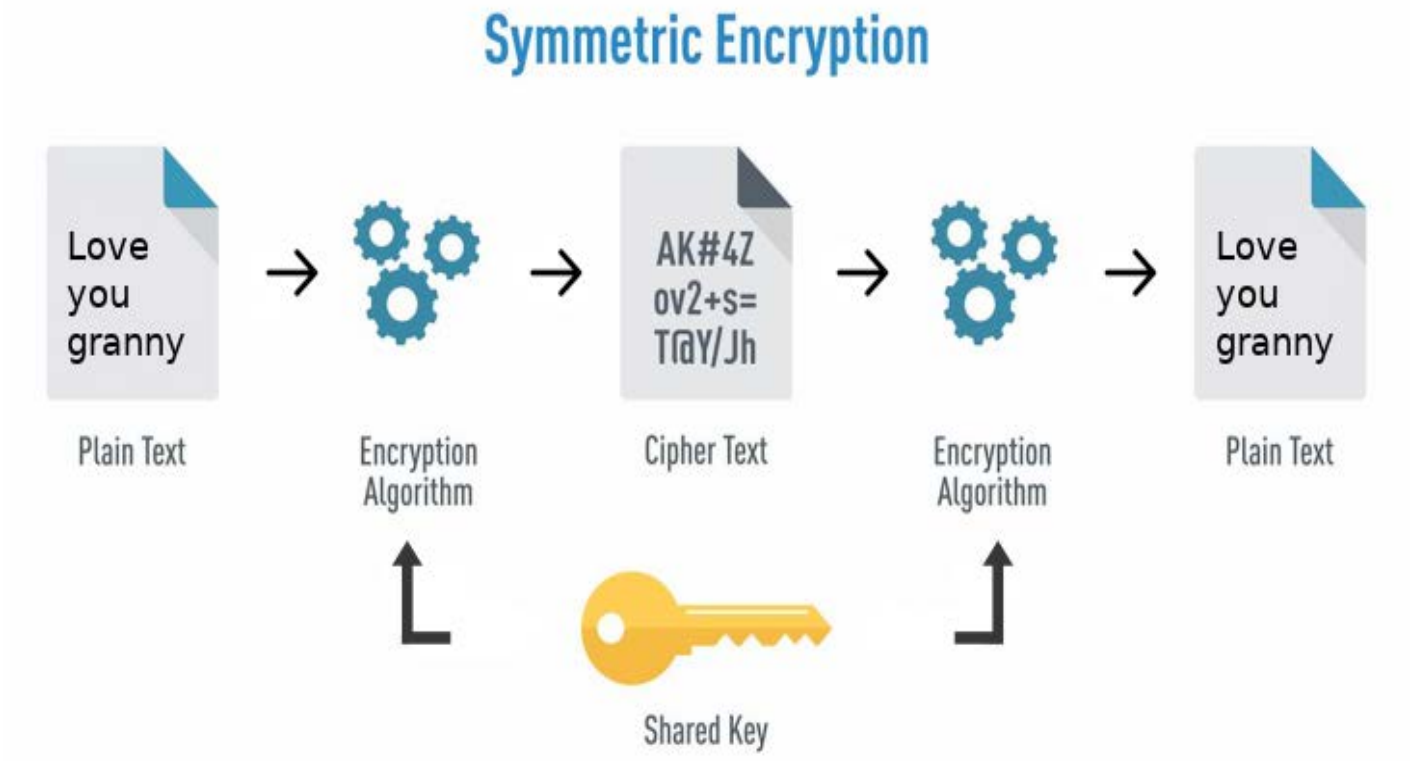

Figure 1 : Symmetric Key Cryptography

B. Asymmetric key cryptography

In this type of encryption, there are two types of keys: the public key and the private key. Both are used in encryption and decryption. The public key is available to everyone.

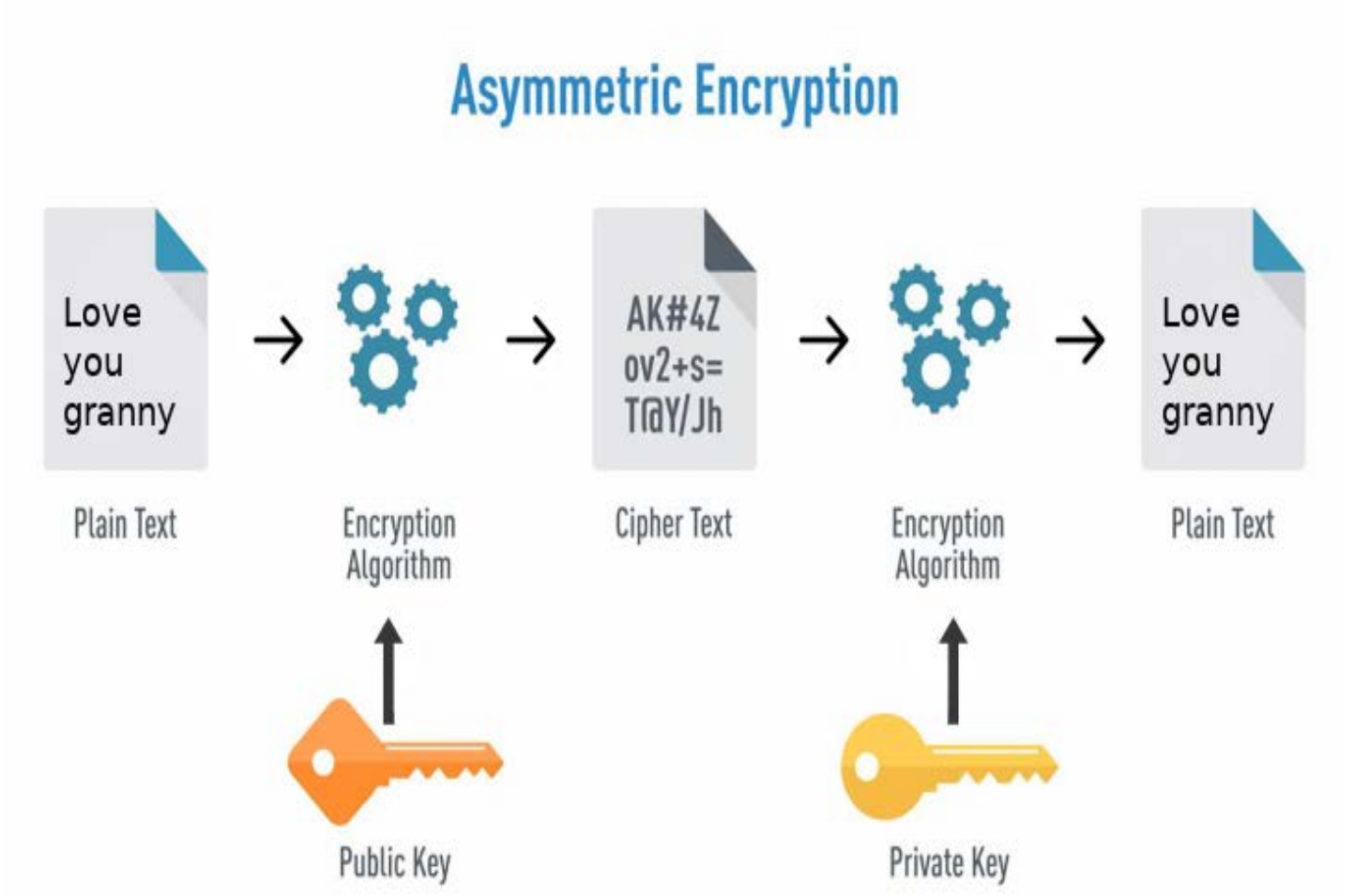

Figure 2 : Asymmetric Key Cryptography

The encryption of the image is done to guarantee the safe transfer of images on the Internet. The encryption mechanism is widely used in this area of image / video transfer, since it does not provide access to unauthorized access. Encryption is also applicable in military communications and telemedicine. Up to the future point of view, the encryption has a greater scope. In the case of image security, the image contains large data, such as high frequency, large capacity and high pixel correlation. The techniques used in encryption can be considered as a tool to protect confidential data. Encryption is a mechanism that can be converted into encrypted or protected data, and can only be read by deciphering it. The process of reverse encryption is known as decryption, which uses a cryptographic key to decrypt the original data. Data encryption has become the best choice for all confidential data, including through the Internet, external networks or internal networks. Encryption is done by applying a mathematical function that generates a key later, and the key is used to obtain the encrypted data. Again, the mathematical key obtained is used for the original data. Security Manager is used to authenticate the user and accuracy in data security [8].

Image encryption is a technique used to hide data or secure image information. This is one of the most common methods that use secure image data. In this way, the image is encrypted and the encrypted image differs from the original image. The encrypted image shows no part of the original image. To obtain the original image from the encrypted image, it has been decrypted.

3. Image Encryption Techniques

There are various types of image encryption technique some of them are describe below:

A. Advanced Encryption Standard (AES)

AES is a symmetric key encryption technique. The secret key is known by the sender and the recipient. This is an iterative encryption instead of Feistel. It is based on a substitution permutation network. The design of the AES algorithm supports the use of one of the three key sizes (Nr). AES 128, AES-196 and AES-256 use respective key sizes of 128 bits (16 bytes, 4 words), 196 bits (24 bytes, 6 words) and 256 bits (32 bytes, 8 words). It consists of a sequence of related operations, some of which involve the replacement of inputs with specific outputs (substitutions) and others involving the mixing of bits (permutations) in dedicated hardware. The AES allows an even faster execution because the transformation of the loop is parallel by design [5].

B. Data Encryption Standard (DES)

The data encryption standard is a symmetric key algorithm for the encryption of electronic data. The data encryption standard is a block encryption. One of the changes that occurred was that which is designed to improve the import of differential cryptanalysis, a cryptographic key and the algorithm uses a data block moderately than a bit at a time. The use of the same key to encrypt and decrypt a message. The DES has been the intention of many attacks for a long time. Some of these attacks analyze the results reduced and promoted in full. The most known were differential cryptanalysis and linear cryptanalysis. Entries in the encryption function: the flat text to be encrypted and the key. In this case, the plain text must be 64 bits long and the key is 56 bits long. This is done through a phase that consists of 16 rounds of the equivalent function, which involves permutation and substitution functions. The 64 entries in the permutations table contain a permutation of the numbers from 1 to 64. Each entry in the permutations table designates the position of a numbered input bit in the output that also consists of 64 bits.

C. ANN Based Approach

The simplified biological neuronal system is known as the Artificial Neural Network, which is connected to the wide range of neurons that treat the elements of the brain nerves. try to partially capture some of your computing power. A neural network includes components such as an activation state vector, an activity aggregation rule, neurons, a connectivity model, an activation rule, a signal function, a rule of thumb. learning and an environment. ANs are taken into account for the high-speed computing environment.

D. Genetic Algorithm (GA)

Genetic algorithms simulate the process of biological evolution using the survival principle of the fittest. GAS has been used for a variety of optimization problems, such as image fragmentation include the extraction of remote sensing and extraction of medicinal properties [7]. In contrast to the traditional improvement methods, GA uses the parallel random

search to arrive at the optimal solution as well they are less likely to stagnate at the local maximum. In each new generation of population it is the values of birth and fitness for all individuals are evaluated in terms of performance in the problem area. The process of selection, crossing and mutation is it is repeated until offspring are produced with an acceptable aptitude value.

The General Assembly will randomly examine the area of candidate solutions to determine The best (or at least sufficient) solution for a particular problem. The fitness function is used to evaluate people and compare them based on the physical fitness score. This result of aptitude the selection process is used to determine which individuals can reproduce and propagate their genes are good for future generations using choice, crossing and mutation.

E. Rivest Shamir Adleman (RSA) Algorithm

RSA operations can be divided into three detailed steps; Key generation, encryption and decryption. The design of the RSA has many flaws. It is therefore not preferred for commercial use. When small p & q values are selected for key design, the encryption process becomes too weak and it is possible to decrypt the data using unspecific probability theory and side channel attacks. It is the most accepted and asymmetric key cryptographic algorithm. It is used in the digital signature. Use the prime number to generate public and private keys based on mathematical facts and simultaneously multiply large numbers.

4. Conclusion

In this paper, many important encryption techniques have been introduced and analyzed to become familiar with the different encryption algorithms used to encrypt the image that has been transferred to the network. According to the survey of recent research, it has been said that security is the main concern in the transmission of images. The security problem is increasing rapidly with tools developed for hacking image data. Many researchers have proposed solutions to the security problem, but have not been able to obtain complete security on the unsecured network.

5. References

1. Ms.Anuradha, Dr. Somesh Kumar, (Prof)Dr.Anuranjan Misra and Dr.K.Rama Krishna, " Improved Rapid AES for Secure Digital Images", IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017), PP-1429-1431, 2017.
2. H.Abood, “An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms”. IEEE Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017) 7 - 9 March 2017.
3. Madhu B., Ganga Holi and Srikanta Murthy K, “An Overview of Image Security Techiques”, International Journal of Computer Applications, Volume 154 – No.6,pp-37-46, November 2016.
4. Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its Growth", Advance in Electronic and Electric Engineering, Volume 4, Number 2, pp. 179-184, 2014.
5. Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan “A Novel Image Encryption Algorithm using AES and Visual Cryptography”, Next Generation Computing Technologies (NGCT), 2016 2nd International Conference of IEEE 2017.

6. Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its Growth", Advance in Electronic and Electric Engineering, Volume 4, Number 2, pp. 179-184, 2014.
7. Vishal Goar, Shikha Mathur, Deepika Gupta and Manoj Kuri, “Analysis And Design Of Enhanced RSA Algorithm To Improve The Security”, 3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT 2017), pp-1-5, 2017.
8. Ujjwal Maulik, “ Medical Image Segmentation using Genetic Algorithms”, IEEE Transactions on Information Technology in biomedicine, Vol-13, No.- 2, pp- 166-173, March 2009.
9. Qi Zhang and Qunding, “Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm”, IEEE Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp-1219-1221, 2015.