RESEARCH ARTICLE OPEN ACCESS

A Review on Different Symmetric and Asymmetric Cryptography Techniques for Digital Image Security

Vijay Kumar Parewa [1], Raj Kumar Sharma [2], Gori Shankar [3]

[1] M.Tech Student, [2] Assistant Professor, [3] Assistant Professor,
Department of Electronics & Communication. Jaipur Engineering College, Jaipur, Rajasthan - India

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. In today on going age to secure the digital image steganography and cryptography techniques are most popular. In cryptography techniques the image is change into one form to totally differ another form. In cryptography different types of algorithm and techniques are used. The algorithm and technique of cryptography is divided into two categories that are symmetric and asymmetric key cryptography. In this paper present the different types of the symmetric and asymmetric cryptography techniques that are very useful to secure the digital image from the unauthorized person or source.

Keywords :- cryptography, asymmetric key cryptography, asymmetric key cryptography, AES, RSA, GA, SVD.

I. 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 [1]. 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 [2].

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 [3]. 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 [4].

II. IMAGE CRYPTOGRAPHY

In image cryptography mainly two terms are used image encryption and decryption. 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 decrypt information in the form of data and images [5].

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 [6].

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. 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 [7].

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.

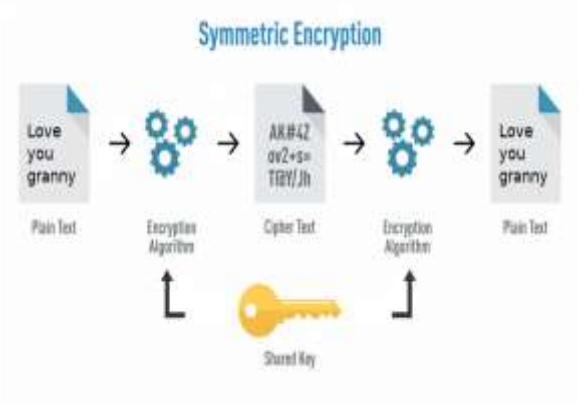

Fig 1 : Symmetric Key Cryptography

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.

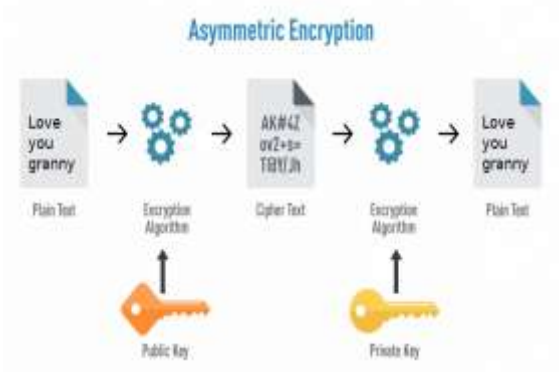

Fig 2 : Asymmetric Key Cryptography

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.

III. IMAGE CRYPTOGRAPHY TECHNIQUES

There are various types of image cryptography 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 [1].

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 (GA) are important non-biased breeding techniques that are used in large area solution tests. Odd random sampling can be used for rapid adaptation in image processing applications. Google Analytics uses images to classify, classify, optimize, extract features and generate images [9].

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. 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.

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 [10-11].

IV. CONCLUSIONS

In this paper, symmetric and asymmetric types of the cryptography techniques are discussed that are very useful to secure the digital data or image from the unauthorized person or attacker. 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. In symmetric and asymmetric algorithm the asymmetric cryptography techniques given the better security then others and in asymmetric cryptography technique RSA is one of the best algorithm to secure the digital.

REFERENCES

[1] Matted S., Shankar G., Jain B.B., “Enhanced Image Security Using Stenography and Cryptography”, Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 58, 2021. Springer, Singapore.

[2] Vipin Singh, Manish Choubisa and Gaurav Kumar Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering & Management, vol. 83, pp. 30561-30565, May-June 2020.

[3] Arpita Tiwari, Gori Shankar and Dr. Bharat Bhushan Jain, "Digital Image And Text Data Security Improvement Using The Combination Of Stenography And Embedding Techniques”, Design Engineering, Issue-7, PP. 8592- 8599, 2021.

[4] Arpita Tiwari, Gori Shankar and Bharat Bhusan Jain, "Comparative Analysis of Different Steganography Technique for Image Security", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 2, pp. 6-9, Mar-Apr 2021.

[5] Himanshu Arora, Manish Kumar and Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167-6177, 2020.

[6] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 IEEE 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[7] Dr. Harish Nagar Manish Kumar, Dr.Sunil Kumar, “Comparative Analysis of Different Steganography Technique for image or Data Security”, International Journal of Advanced Science & Technology (IJAST), Vol-29, Issue-4, 2020.

[8] Manish Kumar, Dr. Sunil Kumar, Dr. Harish Nagar. (2021). Enhanced Text and Image Security Using Combination of DCT Steganography, XOR Embedding and Arnold Transform . Design Engineering, vol-3, pp. 732 – 739, 2021.

[9] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing, pp. 483-492, 2020.

[10] Swati Bhargava, Manish Mukhija, “Hide Image And Text Using LSB, DWT and RSA Based On Image Steganography”, ICTACT Journal on Image & Video Processing, vol-9, issue-3, 2019.

[11] Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.