IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

A Review on Various Image Encryption Technique using AES and Random RGB Substitution

Dharna Singhai[1], Chetan Gupta[2]

M.Tech Scholar, PG Dept. of CSE, SIRTS, Bhopal[1]

Assistant Professor, PG Dept. of CSE, SIRTS, Bhopal[2]

Abstract: Security is the major concerns when the transmission of the data is perform over the network because intruders/attackers of the network steal most of the information from it. So before transmission of the data sender must make secure it by using some of the encryption techniques from the various security techniques available such as DES, AES, MD5, SHA etc. Most of the encryption technique uses secret key to prevent the data from an unauthorized access. In this paper we have discussed various encryption algorithms after study various researches paper and also compare them. Here we suggested AES Encryption algorithm with RGB substitution techniques for the encryption of our data. To provide the strength of our algorithm hidden key is also sent along with data which solves the problem of key exchange which arises in encryption techniques.

Keywords: Hidden Key, Intruders, Symmetric key, Asymmetric key, Encryption, Decryption, AES, DES, MD5, SHA, RGB

I. INTRODUCTION

In today's world, Security is important factor for data storage and transferring of data on public network. We can use cryptography to maintain our files and communication secure. The cryptography is the art and science of encrypting the data in such a way that no-one apart from the sender and intended recipient even realizes the original data, a form of security through obscurity. Image is one of the most important information representation styles and is widely used in many applications like military communication, telemedicine, medical images, etc. Images are often exchanged between two parties over insecure networks [1]. Therefore, the protection of image data from intercepting, copying, and destruction has become a hot problem studied by experts and researchers. Image encryption is the process of realigning the original image into an incomprehensible one that is non-recognizable in appearance, disorderly and unsystematic The swift emergence of the network communication and extension mechanisms in modern era, the demand for security in data reposition and transmission of confidential data in the form of digitized images over the network medium and as a result of increasing in great implication. The distinctiveness of digital images constitutes bulk data capacities and efficient correlations among the neighboring pixels. Conventional encryption procedures like Data Encryption Standard (DES), Advanced Encryption Standard (AES) and the international data encryption algorithm (IDEA) under the private and public key principles are not desirable for the digital image encryption, peculiarly for high speed and real-time applications. In recent years, various encryption schemes have been reported, such as DES, IDEA or AES. However, these schemes have been invented to text or bit

encryption and appear not to be ideal for image applications due to some intrinsic features of images such as the high correlation between neighbor pixels and the high redundancy [2]. Conventional encryption algorithms may not be sufficient to hide these features which can still be visually and statistically apparent even after Encryption nowadays, information always plays a vital role in social communication. To deliver information, people utilize images, sounds, texts and videos to express what they want the others to know. Among these ways, the image is so popular for its authenticity and intuitiveness. With wide use of the images, especially the ones transmitting on the Internet, security of the images has become an imperative problem to deal with. Image encryption is an effective method to protect images by transforming them into an unrecognized format [3].

II. LITERATURE SURVEY

In 2017 May H. Abood [01] proposed an efficient image cryptography using hash-lsb steganography with rc4 and pixel shuffling encryption algorithms in this ensure the encryption and decryption using RC4 stream cipher and RGB

pixel shuffling with steganography by using hash-least significant Bit (HLSB) that make use of hash function to developed significant way to insert data bits in LSB bits of RGB pixels of cover image The results show that high level of the similarity exists between the stego-images and cover images and the same is for secret images and extracted image as represented also in In Histogram Analysis of secret images. These algorithms are performed by using MATLAB program.

In 2017 Jannatul Ferdush, Mahbuba Begum, Ashiq Mahmood [4] proposed a new image encryption method based on displacement of RGB value with one time pad. Any 3D image can be encrypted using this method. The result shows that the proposed algorithm has large key space. So it can resist brute force attack as well as other attacks.

In 2015 Shanthi, Dr.V.Palanisamy [5] proposed method extends such that, the user given plain text is divided into blocks that are fed to the AES Rijndael encryption process, converted to unreadable format. Each character of the block is then shifted into ASCII value which is, in turn formulated into equivalent color code. Thus, the final encrypted text is in image format which make available for more enrichment to the data. The AES algorithm is chosen for its quick and legible conversion of data. Their proposed method is very flexible technology for 256 ASCII values that is converted into 256 color code.

In 2012 Ahmad Abusukhon and Mohammad Talib [6] proposed a simple and a novel data encryption algorithm based on encrypting a text into a white page image (White-Page Image Encryption Algorithm or the WPI algorithm). In this paper, the proposed White-Page Image Encryption Algorithm is tested and analyzed.

In 2012 Praveen.H.L , H.S. Jayaramu, M.Z.Kurian [7] Developed a model which can easily encrypt the images obtained from satellites. Even If faulty data occurs then satellite needs not to wait for long time to receive next data. To prevent this error free encryption scheme is proposed in On-Board. They also states that AES provides an error-free encryption system and error is much more reduced even in radiation in satellites.

In 2012 Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush[8] Employed an AES algorithm to encrypt image, they have first rotated the plain image to generate another image with the help of magic cube. The original image is divided into six sub-images and these sub-images are divided amongst a number of blocks and attached to the faces of a Magic Cube and to confuse the relationship between the plain image and the encrypted image, the rotated image is fed into an AES algorithm which is applied to each pixel of the image to encrypt the image.

In 2012 Jawad Ahmad and Fawad Ahmed [9] had compared two encryption algorithms namely Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). They have explored the security estimations of AES and CFES for digital images against brute-force, statistical, and differential attacks, the results they have calculated to test the security of these algorithms for digital images shows some weaknesses in CFES. These weaknesses were mainly related to low entropy and horizontal correlation in encrypted images, the authors also states that the image encrypted by CFES has correlation in horizontal direction while AES encrypted image has very less correlation in all directions. The algorithm which has less correlation values indicates that it has higher security.

In 2012 Manoj. B, Manjula N Harihar[10] also states that Image Encryption and Decryption using AES can be designed and implemented to protect the confidential image data from an unauthorized access the authors found that Successful implementation of AES algorithm is one of the best encryption and decryption standard available in market

In 2012 P. Radhadevi, P. Kalpana[11] has also presented the encryption and decryption of an image using AES algorithm, they have concluded that the AES can be used very efficiently to secure image transmission.

In 2011 P.Karthigaikumar ,Soumiya Rasheed[12] has also used AES algorithm for simulation of image encryption they have successfully implemented the AES algorithm in MATLAB on Xilinx platform, Timing simulation is also performed which verifies the functionality of the designed circuit.

In 2016 Priya Deshmukh [13] proposed an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output. The AES algorithm for image encryption and decryption which synthesizes and simulated with the help of MATLAB software.

In 2016 Sadhana Singh, Ashish Agrawal and Priyanka Pradhan [14] In this paper novel Advanced Encryption Standard (AES) encryption image schemes based on secret key cipher block and BitMap (BMP) image file format are

proposed. We have to encrypt or decrypt any data or image for providing the network security. This paper simply describes the images protection when we transmit from one place to another. AES encryption technique is one type of selective encryption. The AES algorithm is always worked with the Cipher Feedback mode. While transferring the image from one place to other, there is a problem occurred with the size of the image or the resolution of the image, in this condition we simply compress the image by using the lossless image compression technique. In this paper, we use the Huffman lossless image compression technique for compressing the image which is generated by the text to image encryption. In this paper, we take a text and convert it into image with C# for providing the network security.

In 2017 M.P. Priyanka, E. Lakshmi Prasad, Dr. A. R. Reddy [15] Image encryption and decryption algorithm implemented by using AES 128-bit core. Here, image information is converted into a hexadecimal format using Matlab code and this plain hexadecimal data are transmitted to the FPGA via UART for encryption. Thus, the same process is also used for Decryption. The entire AES 128-bit core is simulated and synthesized for Spartan-3E-1600E FPGA using Xilinx ISE 14.3. Therefore, the experimental results are measured and compared with respect to area, power, and latency. The total amount of area occupied for encryption is 6% of slices, 2% of slice Flip flops, 5% of 4-input LUTS and 44% of BRAMS, latency for 128-bit is 6.645 ns and the amount of power consumption is 441.91 mW. Similarly, for the decryption amount of area occupied is 7% of slices, 2% of slice Flip flops, 7% of 4-input LUTS and 55% of BRAMS, latency for 128-bit is 7.770 ns and the total amount of power consumption is 442 mW.

In 2017 Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan [16] proposed a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image. The image is encrypted using AES and an encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing. The cryptanalysis of the algorithm is then performed and is proved to be secure.

III. EXISTING TECHNIQUE

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 to both the sender and the receiver it is an iterative rather than Feistel cipher. It is base on substitution–permutation network. The design of AES algorithm supports the use one of any three key sizes (Nr). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. It comprises of a sequence of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations) in dedicated hardware AES allows even faster execution as the round transformation is parallel by design.

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 cipher. One of the changes that occur was that DES is specifically designed to resist differential cryptanalysis import a cryptographic key and algorithm are applied to a block of data simultaneously moderately than one bit at a instant. DES works by using the same key to encrypt and decrypt a message, The DES has been a intention for many attacks for a long time. Some of these attacks started by analyzing reduced-rounds DES and went up to the full-round DES. The most known were differential cryptanalysis, and linear cryptanalysis. DES is two inputs in the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in the length and the key is 56 bits in length. This is following through a phase consisting of 16 rounds of the equivalent function, which involves both permutation and substitution functions. The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table designates the position of a numbered input bit in the output which also consists of 64 bits.

c. Rivest–Shamir–Adleman (RSA)

RSA operations can be decayed in three extensive steps; key generation, encryption and decryption. RSA have many flaw in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using unsystematic probability theory and side channel attacks. It is most accepted and asymmetric key cryptographic algorithm. It is used in digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers simultaneously.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Fig.1 shows the encryption decryption process, here some of the major terms that are commonly used in this process are as follows:

Plain text: plain text is used as input to an encryption algorithm it is an original text.

Cipher text: It is a coded message Cipher is an algorithm to plain text to get cipher text.

Encryption: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it in this we can convert our original plain text into cipher text.

Decryption: Decryption is the process of taking encoded or encrypted text or other data and converting it back into plain text. It may also be performed with a set of keys or passwords.

Public Key- Public-key encryption is a cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message.

Private Key- A private key is a tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption. A private key is also known as a secret key.

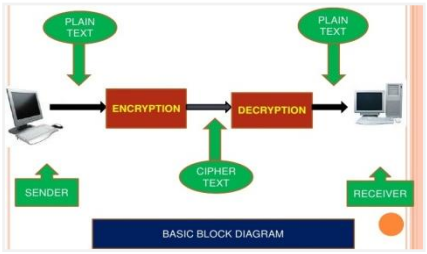

Fig.1 Process of Cryptography

IV PROBLEM DOMAIN

The gaps identified from this survey and analyses are as follows:

1.Previous algorithm fails to work on multi image encryption.

2. It may be very safe for image encryption applications, and outperforms the competitive encryption and decryption techniques are needed for better security.

3.Information loss is very high in encryption and decryption in previous approach.

4. It has large key space and outperforms the competitive image encryption algorithms in terms of efficiency.

5.No use of hide color image in other color image as future consideration.

6.Multiple keys randomization is needed for secure the password.

7.Proper XOR not operated in the middle to shuffle the data and rearrangements.

8.Data hiding techniques with bit shuffling can be applied for enhancing the security Key length can be expanded so that it can enhance the key security as compared to the traditional techniques.

V. ANALYSIS

S. No	Approach	Information Accuracy	Information accuracy after Encryption
1	SPN structure [18]	Leena Image 7.5534	7.9669
2	PSNR Comparison [18]	Clown Image 32.52	Clown Image 39.43
3	Block Based Transformation on [19] Proposed technique 30 × 30	0.0063	5.4402
4	Block Based Transformation on [19] Proposed technique 100 × 100	0.0044	5.5407
5	Chaotic System Lena image[20]	7.5534	7.9669
6	Chaotic System Circle image[20]	6.0408	7.9652

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

VI. PROPOSED ARCHITECTURE

This section, describes the proposed encryption algorithm. This technique is designed to improve the algorithm proposed by the Ahmad Abusukhon and Mohammad Talib [6]. First of all their algorithm does not solve the key exchange process. Another loop hole is that they have to transfer the whole key, this is quite big in size (key1) as every character in plain text has been replaced by three random numbers. Hence it requires transferring at least three times more data as compared to actual data just for decrypting the packet. Fig.3 shows the block diagram of proposed technique. Since encryption is better option as compared to simple shuffling of bits, hence proposed technique employs an encryption stage rather than shuffling the bit positions by matrix scrambling technique [14]. The sender & receiver side has a combination database that contains various combinations of text to digit mapping. It has various for transforming characters into equivalent RGB values, where each combination is assigned a unique number ranging from 1 to N where N denotes the total number of combinations. Now starting from the sender side, the sender generates a random number between 1 to N, which represents the combination number to be applied. Using the corresponding combination, transformation proposed in [6] is applied for generating the resultant image. Now this image is encrypted by a key using an AES algorithm [15], which generates an encrypted image. On this encrypted image, one more pixel is added, which stores the value of the combination number that was used to transform text into the image. Now the key which was used in AES algorithm is transformed to its equivalent RGB resultant value. Finally these resultant values and the final image generated are transferred to the destination host. Upon receiving the final image, the first task is to read the last pixel that was added to get the combination number. Once this number is obtained the received key is transformed to its original value by using the combination number. After this, corresponding transformation is applied with the help of various combination databases. Now receiver discards the last pixel from the image and then applies AES on image (using previously obtained key), which was generated after discarding the last pixel. When receiver obtains the decrypted image it applies the transformation with same combination number that was found in the last pixel of received image and generates the original text. Fig. 2 shows the all phases of AES Algorithm.

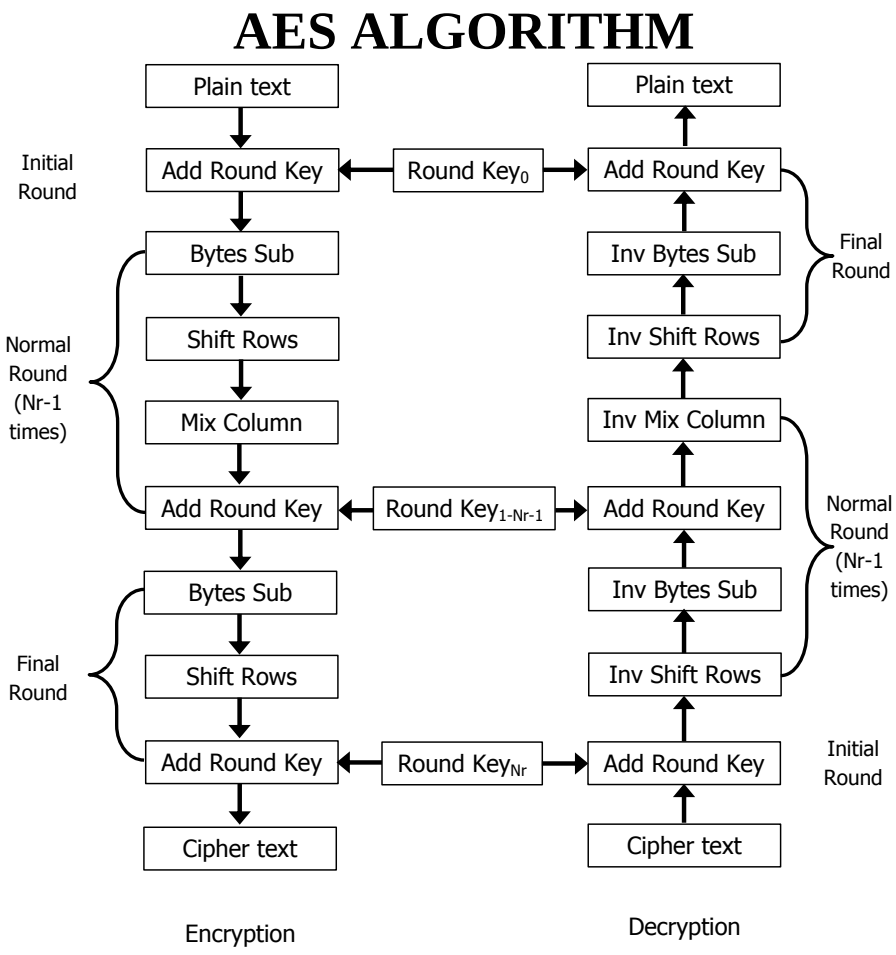

Fig.2 Block diagram from AES Algorithm

VII. CONCLUSION AND FUTURE WORK

It is very essential to prevention the data from the unauthorized access. In this paper we study some of the existing encryption techniques additionally recommend the use of AES encryption algorithm as fast in nature for encryption and decryption along with some pixel shuffling technique so this hybrid combination make our system more secure to transmit out secret information over a network or computer network this system will result the more strength and less information loss after encryption and decryption process.

REFERENCES

[1] H.Abood, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms". Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017) 7 - 9 March 2017 IEEE.
[2] Komal D Patel, Sonal Belani "Image Encryption using different Techniques" International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 1, November 2011.
[3] Nooka Saikumar, R. Bala Krishnan, S.Meganathan, N.R. Raajan, "An Encryption Approach for Security Enhancement in Images using Key Based Partitioning Technique" International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE 2016.
[4] Jannatul Ferdush, Mahbuba Begum, Ashiq Mahmood "A New Image Encryption Technique Combining the Idea of One Time Pad with RGB Value" International Journal of Computer Applications (0975 – 8887) Volume 178 – No.5, November 2017
[5] Shanthi, Dr.V.Palanisamy "A Novel Text to Image Encryption Technique by AES Rijndael Algorithm with Color Code Conversion", International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 5 – Jul 2014.
[6] Ahmad Abusukhon Mohammad Talib "A Novel Network Security Algorithm Based on Private Key Encryption" IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 .
[7] Praveen.H.L, H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" International Journal of Computer Science and Electrical Engineering (IJCSEE), Vol-1, Iss-2, 2012.
[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm" International Journal of Computer Science Issues (IJCSI); Vol. 9 Issue 4, p41 Jul2012.
[9] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04, 2012
[10] Manoj.B, Manula N Harihar "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[11] P. Radhadevi, P. Kalpana "Secure Image Encryption Using AES" International Journal of Research in Engineering and Technology Volume: 1 Issue, 2012
[12] P.Karthigaikumar Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on Computational Science - New Dimensions & Perspectives" NCCSE, 2011.
[13] Priya Deshmukh "An image encryption and decryption using AES algorithm", International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518.
[14] Sadhana Singh, Ashish Agrawal and Priyanka Pradhan "Advanced Text to Image Encryption by Using Selective Encryption Technique with C# (AES Encryption and CFB Mode)", International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2016.
[15] M.P. Priyanka, E. Lakshmi Prasad, Dr. A. R. Reddy "Fpga Implementation Of Image Encryption And Decryption Using AES 128-Bit Core", In proceeding of IEEE explore 2017.
[16] 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.
[17] Kiran Kumar, M., Mukthyar Azam, S., and Rasool, S."Efficient digital encryption algorithm based on matrix scrambling technique". International Journal of Network Security and its Applications (IJNSA), 2010.
[18] Seetaiah Kilaru, Yojana Kanukuntla, K B S Chary," An effective algorithm for Image security based on Compression and Decomposition method", International Journal of Advanced Computer Research (ISSN (IJACR) Volume-3 Number-1 Issue-8 March-2013.
[19] Mohammad Ali Bani Younes and Aman Jantan," Image Encryption Using Block-Based Transformation Algorithm", IAENG International Copyright to IJARCCE.
[20] Long Bao, Yicong Zho, C. L. Philip Chen, Hongli Liu, "A New Chaotic System for Image Encryption" International Conference on System Science and Engineering, June 30-July 2, Dalian, China IEEE 2012.