International Journal for Modern Trends in Science and Technology, 8(09): 116-118, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809022
Available online at: http://www.ijmtst.com/vol8issue09.html

Utilizing the AES Technique for Image Encryption

V.Hima Maheswari[1] | P.Srinivas Reddy[2]

[1]PG Scholar, Department of Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
V.Hima Maheswari and P.Srinivas Reddy. Utilizing the AES Technique for Image Encryption. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 116-118. https://doi.org/10.46501/IJMTST0809022

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

Nowadays almost all virtual services like internet communication, clinical and navy imaging structures, multimedia system calls for reliable protection in storage and transmission of digital pictures. due to faster growth in multimedia technology, net and cellular telephones, there is a want for security in virtual pictures. therefore there may be a want for picture encryption techniques in an effort to disguise pictures from such assaults. on this system we use AES (superior Encryption approach) a good way to hide picture. Such Encryption method facilitates to avoid intrusion assaults. The resistance of AES closer to differential and linear cryptanalysis comes from a higher "avalanche effect" (a piece flip sooner or later quickly propagates to the whole inner nation) and specifically crafted, bigger "S-boxes" (a S-container is a small lookup desk used in the algorithm, and is an easy way to feature non-linearity; in DES, S-packing containers have 6-bit inputs and 4-bit outputs; in AES, S-boxes have 8-bit inputs and 8-bit outputs).

Keywords: AES,Block cipher,cryptography,DES,NIST.

1. INTRODUCTION

The observe of photograph cryptography has been a charming area of research, in the recent beyond, in view of its importance in the transmission of snap shots on the internet. As there are numerous block ciphers available in the literature, many authors committed their attention to encryption of grey level snap shots and colour images. the safety of the statistics accomplished on this manner is pretty commendable, and it performs a extensive position as no outside agent can decipher even a hint of the content material of the photo furnished that the cipher is a sturdy one. In a recent research, Sastry and Shirisha have evolved a novel block cipher which includes a pair of key bunch matrices E and D, where E=[eij],i=1to n, j= 1 to n is the encryption key bunch matrix, and D= [dij], i= 1 to n, j= 1 to n is the decryption key bunch matrix. For every given eij, the corresponding dij is received by the usage of the relation (eij.× dij) mod 256 = 1 here it is to be referred to that both eij. anddij are atypical numbers mendacity inside the c language [1,255]. The primary equations governing the encryption and the decryption of the cipher are given by means of P = [eij × Pij] mod 256, i=1 to n, and j= 1 to n C= mix(P), and C = Imix(C), P = [dij × Cij] mod 256, wherein P is the plaintext and C is the ciphertext which can be written inside the form P = [P ij] and C=[Cij]. inside the cryptanalysis done in , the authors have shown that this cipher is very robust because the binary bits of the

plaintext are very well blended, with the aid of using the mixture() function in each spherical of the iteration method involved inside the cipher. it may be stated right here that the feature Imix() denotes the reverse manner of the mixture(). within the present paper, our goal is to expand a method for the encryption of a grey level picture and a shade photo the usage of the aforementioned block cipher. here our interest is to look how the encryption done by using the cipher definitely transforms the pictures. on this evaluation, we employ the RGB model in wearing out the development of the encryption of the colour picture. In what follows we gift the plan of the paper. ,we address the development of a manner for the cryptography of an picture. we illustrate the cryptography of an photo. Then we speak the encryption of a gray stage photograph , and the encryption of a colour photo in . subsequently, we draw conclusions received from this analysis.

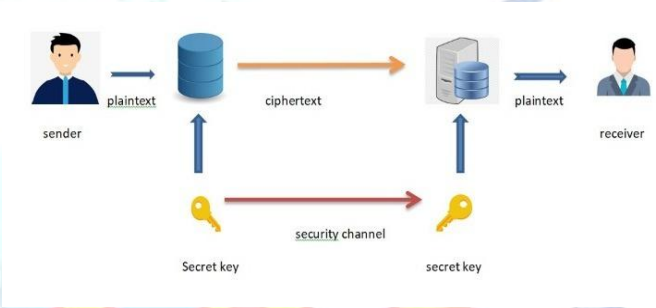
2. LITERATURE SURVEY

Digital image security has become more crucial with the advancement of the Internet technology. Visual encryption technique has many application areas like multimedia, biometrics, image processing, GIS, military communication etc. Various methods have been proposed for secure sharing of the images. One of the techniques based on random pixel permutation is proposed by the author [1] In this technique the values used in the encryption process are preserved in the form of a 64 bit key and sent to the receivers. The receivers jointly use the key and the shares to see the secret [1]. In order to protect digital image from unauthorized user and access, variety of Image encryption techniques have been proposed, one of the techniques is proposed by, Pareek [2] in 2011, to develop a novel image encryption technique using 144-bit secret key. A secret sharing scheme using simple graphical masking with the help of AND and OR operation is proposed in [3]. Further, a new (2n) visual secret sharing scheme for colored images is proposed with hybrid technique by Lee and Le [4]. An image encryption scheme based on generalized logistic map, AES Sbox, cipher text feedback, Piecewise Linear Chaotic Maps is proposed in [5]. The cryptosystem is based on AES S-box, generalized logistic map and cipher text feedback [5].

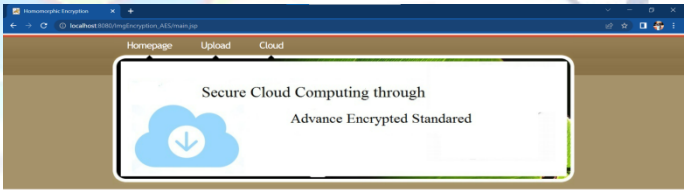
3. PROBLEM STATEMENT

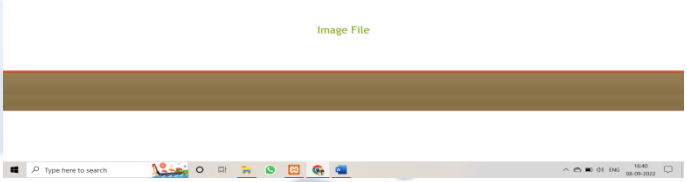
DES (information Encrypted machine) turned into designed with an powerful key duration of fifty six bits, that's at risk of exhaustive seek. It additionally has a few weaknesses against differential and linear cryptanalysis: these permit to get better the key using, respectively, 247 chosen plaintexts, or 243 acknowledged plaintexts. A regarded plaintext is an encrypted block (an eight-byte block, for DES) for which the attacker knows the corresponding decrypted block. a chosen plaintext is a type of regarded plaintext in which the attacker receives to pick out himself the decrypted block.

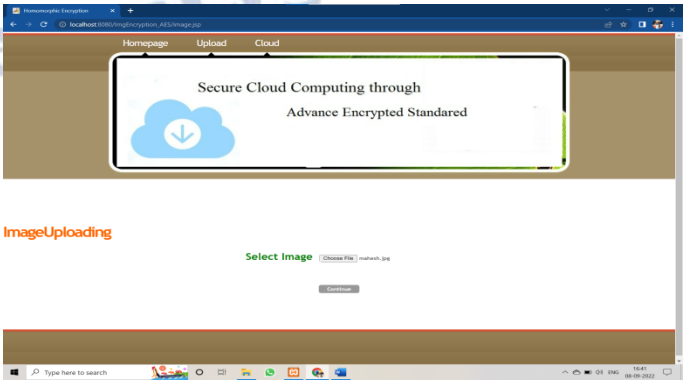
Architecture:



4. RESULTS







5.CONCLUSION

In this analysis, we've studied the encryption of a grey stage picture and the encryption of a colour picture by way of the usage of a block cipher which includes a key bunch matrix. on this matrix, all of the keys are bizarre numbers which lie in the c program languageperiod within the method of the encryption of every portion of the photograph, the iteration scheme present in the block cipher, and the characteristic blend() that is blending the binary bits of the gray degree values are playing a outstanding function in strengthening the encryption of the photo. here it is to be stated that within the case of the grey stage photo, the encrypted photograph incorporates unique mixtures of black and white dots, and it does now not show off any feature of the authentic image. then again, in the case of a color image, the encrypted picture seems as a mixture of RGB shade pieces and it does no longer indicate any courting with the authentic colour picture.

The research paper proposes a gadget which can be used for effective picture data encryption and key generation in diverse software regions, wherein sensitive and exclusive facts needs to be transmitted along with the image. the next step in this course could be machine implementation, calculating time and area complexity for the equal the use of a few experimental data after which evaluating it with current algorithms and schemes for its efficiency, accuracy and reliability.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology, Vol. 27, pp. 206 – 211, 2007.

[2] Xiao Huijuan, QiuShuisheng, Deng Chengliang He Yong-Zhong, Cai Ying, "A Composite Image Encryption Scheme Using AES and Chaotic Series", The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007), pp. 277 – 279, 2007.

[3] Guanrong Chen, Yaobin Mao b, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol. 21, 749 – 761, 2007.

[4] Ashtiyani, M. Birgani, P.M. Hosseini, H.M., "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", Information and Communication Technologies: From Theory to Applications, ICTTA-08. 3rd International Conference on, pp. 1 – 5, Apr 2008.

[5] Zhenzhen Lv1, Lei Zhang2, and JianshengGuo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System", Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09) Huangshan, P. R. China, 26-28, pp. 191-194, Dec. 2009.

[6] Bibhudendra Acharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy, Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.

[7] AbdulkarimAmerShtewi, BahaaEldin M. Hasan, Abd El Fatah, A. Hegazy, "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No. 2, pp. 226 – 232, Feb 2010.

[8] R. Lukac and K. Plataniotis. Bit-Level Based Secret Sharing for Image Encryption. Pattern Recognition, 38(5):767–772, May 2005.

[9] Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images",IEEE International Conference on Image Processing, 2006.

[10] Puech, W.; Rodrigues, J.M.; Bors, A.G.,"Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images", Eighth International Workshop on Image Analysis for Multimedia Interactive Services, 2007. WIAMIS07, June 2007.

[11] V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix", International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, October 2012, pp.1-6.

[12] Alasdair Mcandrew, —Digital Image processing with MatLab, Cengage learning 2004.

[13] Rafael C. Gonzalez & Richard E. Woods,— Digital Image processing, 2ndEdition Pearson Education 2004.

Authors Biography

V.Sai Samyuktha currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. Her research interests include Data Structures, Web Technologies, Operating Systems, Data Science and Artificial Intelligence.

P.Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University. His research interests include Operational, Research ,Probability and Statistics , Design and Analysis of algorithm , Big Data Analytics