GUI implementation of image encryption and decryption using Open CV-Python script on secured TFTP protocol

Conference Paper · August 2018

CITATIONS
0

READS
199

2 authors, including:

Rasool Reddy Kamireddy
VIT University Andhra Pradsh
7 PUBLICATIONS **0** CITATIONS

SEE PROFILE

GUI implementation of image encryption and decryption using Open CV-Python script on secured TFTP protocol

K. Rasool Reddy, and Ch. Madhava Rao

Citation: AIP Conference Proceedings **1952**, 020074 (2018); doi: 10.1063/1.5032036
View online: https://doi.org/10.1063/1.5032036
View Table of Contents: http://aip.scitation.org/toc/apc/1952/1
Published by the American Institute of Physics

GUI Implementation of Image Encryption and Decryption Using Open CV-Python Script on Secured TFTP Protocol

K.Rasool Reddy[1], Ch. Madhava Rao[2]
[1]*Gudlavalleru Engineering College,* [2] *Sir C.R.Reddy College of Engineering*
[1,2]*Andhra Pradesh, India*
[1]*rasoolkamireddy3738@gmail.com,* [2]*madhava_ch@yahoo.com*

Abstract. Currently safety is one of the primary concerns in the transmission of images due to increasing the use of images within the industrial applications. So it's necessary to secure the image facts from unauthorized individuals. There are various strategies are investigated to secure the facts. In that encryption is certainly one of maximum distinguished method. This paper gives a sophisticated Rijndael (AES) algorithm to shield the facts from unauthorized humans. Here Exponential Key Change (EKE) concept is also introduced to exchange the key between client and server. The things are exchange in a network among client and server through a simple protocol is known as Trivial File Transfer Protocol (TFTP). This protocol is used mainly in embedded servers to transfer the data and also provide protection to the data if protection capabilities are integrated. In this paper, implementing a GUI environment for image encryption and decryption. All these experiments carried out on Linux environment the usage of OpenCV- Python script

Keywords. Advanced Encryption Standard, Trivial File Transfer Protocol, Exponential Key Change, OpenCV, Python Script.

INTRODUCTION

Currently the usage of computer systems, internet and wireless communication has been rapidly developing. Presently; hundreds of thousands of peoples switch/exchange the data through a computer network. However, safety is one of critical problem while transferring the data between client and server. There are various strategies are avail to secure data from vulnerable attacks, in that cryptography is one of the most prominent technology in embedded systems.

Generally there are two sorts of algorithms in cryptography: (1) Symmetric Key Cryptography (2) Asymmetric Key Cryptography. In this work, Symmetric Key algorithm is used for encoding (encryption) and decoding (decryption) of information. There are several strategies are avail for Symmetric Key Cryptography like DES, 3DLES, AES, MAES etc. [1-3].

In 1997, the NIST recognized as DES was not secure because of it requires more power to process the data. Due to that, after few years NIST invented a replacement for DES algorithm named as Rijndael algorithm [4]. Later Rijndael algorithm named as AES [5] algorithm.

In this work an efficient cryptographic algorithm such as AES-128 [6] is implemented on secured TFTP Protocol using OpenCV-Python Scripting Language. The below figure 1 shows the iterative block diagram of AES-128 and is adopt from [7].

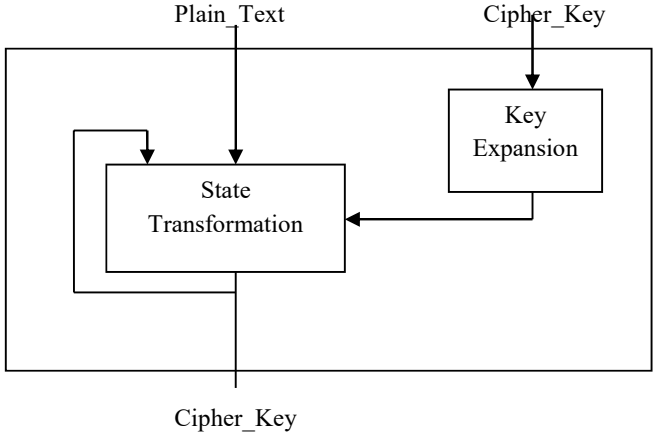

FIGURE 1: AES Block Diagram

International Conference on Electrical, Electronics, Materials and Applied Science
AIP Conf. Proc. 1952, 020074-1–020074-8; https://doi.org/10.1063/1.5032036
Published by AIP Publishing. 978-0-7354-1647-5/$30.00

The rest of the paper organized as: Section 2 deals with the proposed method. Section 3 gives experimental setup and results. In Section 4 describes the conclusion & future scope of proposed work.

PROPOSED METHODOLOGY

The below figure 2 represents the methodology of encryption and description of data between client and server on secured TFTP protocol.

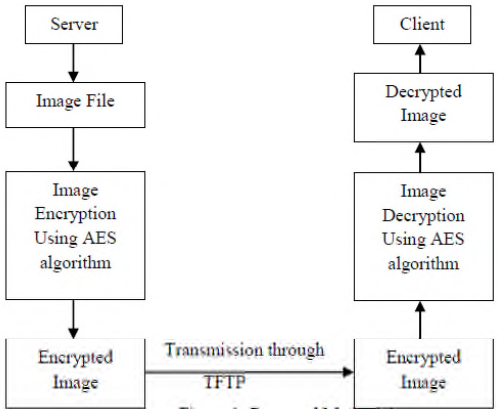

FIGURE 2: Proposed Methodology

Initially the image file is encrypted by AES algorithm and transmits the encrypted image through TFTP protocol from sever to client and finally client decrypted the image using AES algorithm. Here Exponential Key Change (EKE) concept is also introduced to exchange the key between client and server.

Encryption

AES-128 is operating with a key length (N_k) of 4, 6 and 8. Length of block (N_b) is 4 and number of rounds (N_r) depends on N_k. The table 1 represents the number of possible rounds in different techniques.

TABLE 1: Rounds (N_r)

Technique	Rounds (N_r)	References
Rijndael -128	10	[6]
Rijndael -192	12	[8]
Rijndael -256	14	[9]

The below figure 3 represents encryption of AES encryption algorithm. The Rijndael algorithm consists of 3 rounds namely

- First Round
- Rounds (Repeated Rounds)
- Final Round

First Round

In this round perform AddRoundKey operation. In the AddRoundKey simply perform XOR operation round key and a portion of key. This transformation is illustrated in figure 6

Rounds

SubBytes: In this each and every 8bits (byte) is replace with another 8bits according to S-Box. This transformation is illustrate in below figure 4

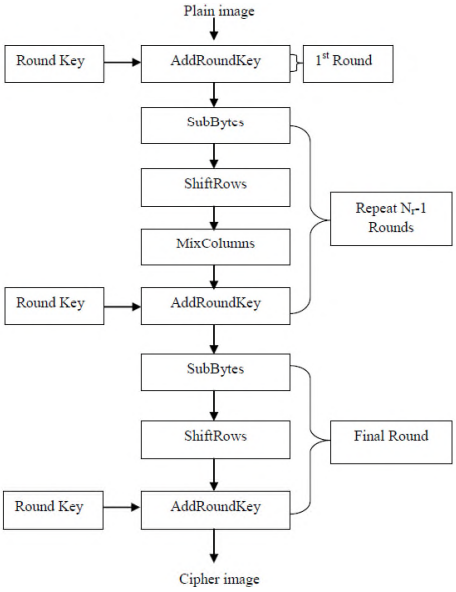

FIGURE 3: Encryption Algorithm

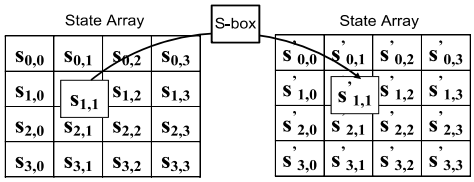

FIGURE 4: SubBytes Transformation

ShiftRows: It is transposition stage and operates on individual rows. The transformation of ShiftRows is shown in below figure 5.

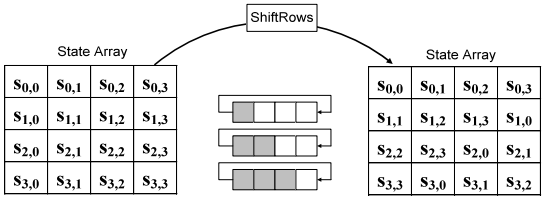

FIGURE 5: ShiftRows Transformations

The below table 2 represents possible number of shifts in ShiftRows for AES-128 encryption algorithm.

TABLE 2: Number of Shifts in ShiftRows

N_b	Row 0	Row 1	Row 2	Row 3
4	0	1	2	3
6	0	1	2	3
8	0	1	3	4

MixColumns: It is operating on the individual column of the state, mix the 32 bits in each column. This transformation is illustrated in below figure 6.

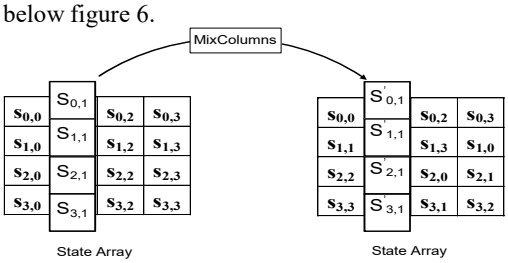

FIGURE 6: MixColumns Transformations

AddRoundKey: In the AddRoundKey simply perform XOR operation round key and a portion of key. This operation shown in below figure 7

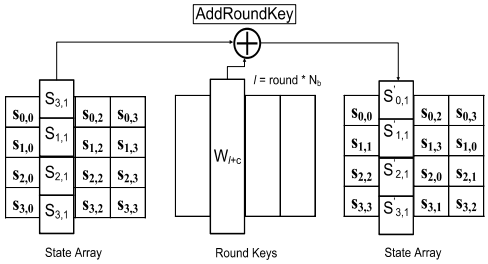

FIGURE 7: AddRoundKey Transformations

1.1.1. Final Round

The final round consist the following operations

- SubBytes
- ShiftRows
- AddRoundKey

The AES algorithm performs Cycles of Repetition (Round) function for its Cipher and inverse Cipher. A set of several reverse rounds are performed to transform Cipher image to plain image using same key. The figure 8 illustrates Pseudo Code for AES cipher.

```
Cipher(byte PlainText[4*Nb], byte CipherText[4*Nb], word w[Nb*(Nr+1)])
begin  byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr–1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

FIGURE 8: AES Cipher

Trivial File Transfer Protocol (TFTP)

The TFTP is a technique to exchange/transfer the data between two computer systems (client and server) on different networks implementing UDP (Datagram) in a closed environment and also provide protection to the data if protection capabilities are integrated. Due to simplicity TFTP lacks most of the features compared to FTP. The TFTP only read/write the files from/to the server. It is also transfer 8-bit bytes of data. The TFTP supports 5 kinds of messages (packets) and is shown is below figure 9.

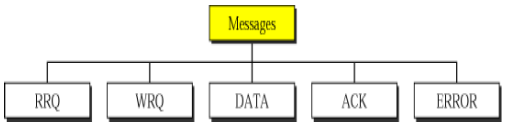

FIGURE 9: TFTP Messages

TFTP Message Format:

The below figure 10 represents TFTP message formats.

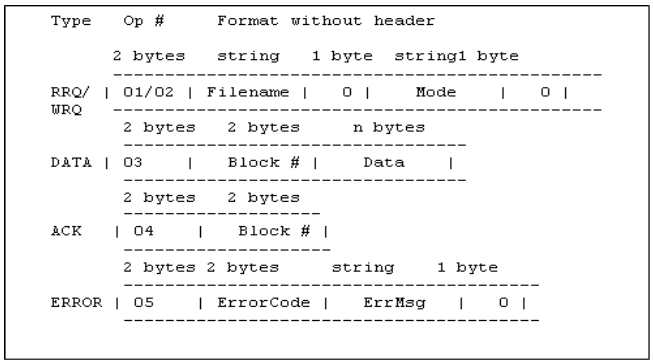

FIGURE 10: TFTP Message formats.

RRQ (Read Request):

The given below figure 11 represents the TFTP Read Request between client and server.

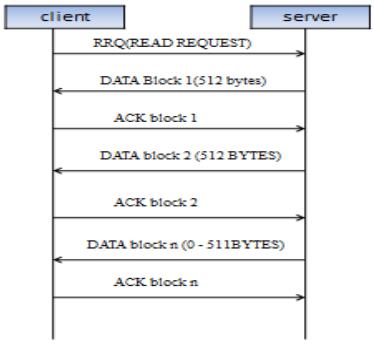

FIGURE 11: TFTP RRQ

WRQ (Write Request):

The given below figure 12 represents the TFTP Write Request between client and server.

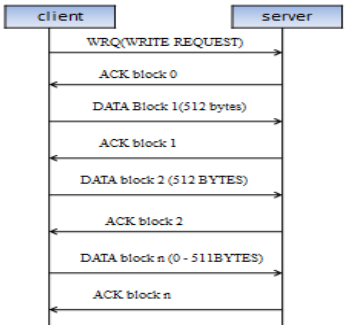

FIGURE 12: TFTP WRQ

In [10-12] proposed the TFTP protocol can't transfer the files of size more than 32Mb. Furthermore, in order to exchange the key over a channel, Exponential Key Exchange (EKE) is also introduced [10]. The purpose EKE is to provide secure key exchange in TFTP.

Decryption

The figure 13 describes the Decryption of data using Rijndael algorithm. The operation of Decryption is inverse of Encryption.

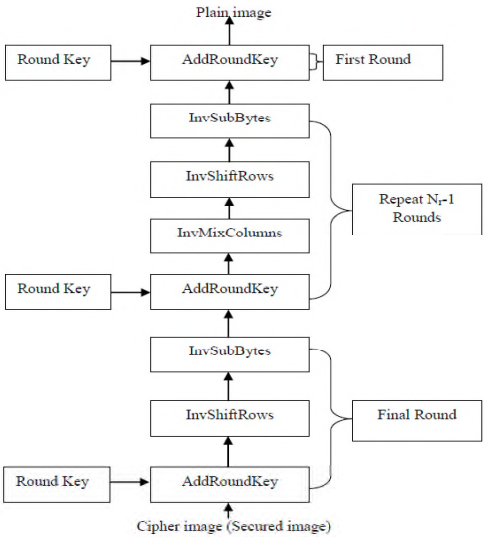

FIGURE 13: Decryption Algorithm

Results and Discussions

An experimental setup is made up of following requirements:
Server: Desktop Intel Dual Core Processor CPU 1.2 GHz
Client: Desktop Intel Xeon® processor CPU E31270 3.4 GHz

Image is transfer through TFTP in LAN using wired router to decrypt. Both client and server are setup on Linux environment and implementing OpenCV-Python script. Here all the images are in .jpg format. The below figure 14 represents the image to be encrypted and decrypted (original image) with a resolution of 512*756.

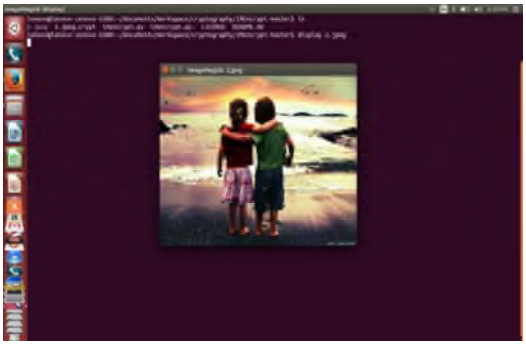

FIGURE 14: Original image

Figure 15 represents the Graphical User Interface of proposed method.

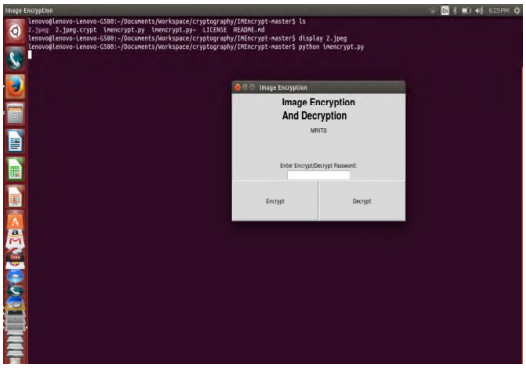

FIGURE 15: Graphical User Interface

The given below figure 16 shows encrypted image message display. The encrypted image stored in the ".crypt" format.

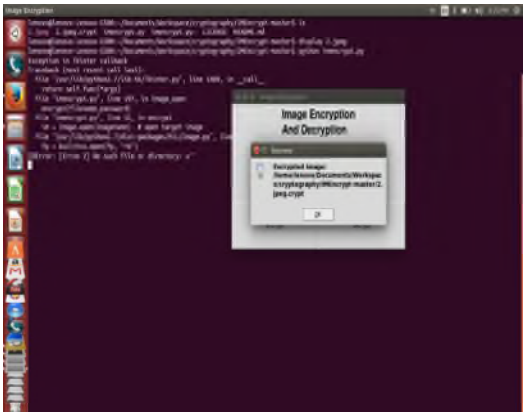

FIGURE 16: Encrypted Image

The given below figure 17 represents the encrypted message of figure 16 and figure 18 represents the decrypted image using AES algorithm.

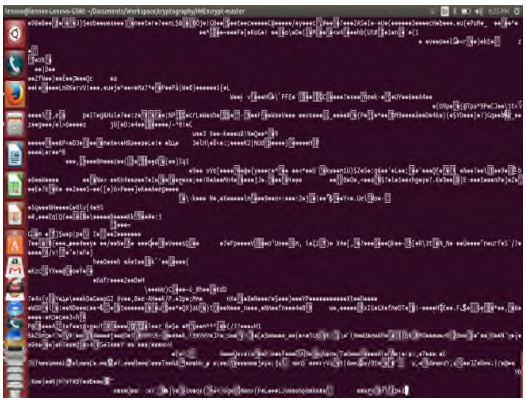

FIGURE 17: Encrypted Message

FIGURE 18: Decrypted Image

CONCLUSION AND FUTURE SCOPE

From the experimental results, we can say that the encryption of image (AES) is one of most prominent technique in order to protect/secure the data and as well as save the time compared to other strategies DES, 3DES. We bring out the cryptographic security implementations in TFTP using EKE for exchange of key and

AES for image encryption and decryption to secure the data from unauthorized third party individuals. In future, this work is extended to Video/Audio encryption.

REFERENCES

1. Abdel-Karim, “Performance Analysis of Data Encryption Algorithms”.
2. Y.Ou , C.Sur , K. H Rhee”Region based selective Encryption for Medical Imaging”,1st Annual International Workshop-2007
3. S. H Kamali, R.Shakerian, M.Hedayati,”A new modified version of Advanced Encryption Standard based algorithm for image encryption”, International Conference on Electronics and information Engineering, ICEIE-2010.
4. Nur Nabila Mohamed, Habibah Hashim, Yusnani Mohd Yussoff, “Compression and Encryption Technique on Securing TFTP Packet”, 2014 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , April 7 - 8, 2014, Penang, Malaysia.
5. H. Trang and N. Loi, "An efficient FPGA implementation of the Advanced Encryption Standard," in Computing and Communication Technalogies, Research, Innavation, and Visian far the Future (RIVF), 2012 IEEE RIVF Internatianal Conference on, March 2012.
6. M.P.Priyanka, E.Lakshmi, Dr.A.R.Reddy, “FPGA Implementation Of Image Encryption And Decryption Using AES 128-Bit Core”, Communication and Electronics Systems (ICCES), International Conference on 21-22 Oct. 2016
7. El Maraghy M, Hesham S and Abd El Ghany M.A, “Real-time Efficient FPGA Implementation of AES Algorithm”, IEEE International SOC Conference (SOCC), Sept 2013.
8.]Monica Lib eratori, Fernando Otero, J. C. Bonadero, Jorge Castifieira”AES-128 cipher. high speed, low cost FPGA implementation”, IEEE-2007.
9. Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, Hung-Yun Tai, “Compact FPGA Implementationof 32-bits AES Algorithm Using Block RAM”, IEEE-2007.
10. N. N. Mohamed, H. Hashim, Y. M. Yussoff, and A. M. Isa, “Securing TFTP packet: A preliminary study,” IEEE 4th Control Syst. Grad. Res. Colloq. Aug. 2013.
11. http://tools.ietf.org/pdf/rfc783.pdf.
12. http://tools.ietf.org/pdf/rfc2347.pdf.