SENIOR PROJECT

CRYPT THE PICTURE

Submitted by:

Eda Daniş & Esma Sert & Havvanur Aydın

Project Supervisor: Assoc.Prof Cafer Çalışkan

Faculty of Engineering

Antalya Bilim University

Spring 2018

FOREWORD

The idea of doing our senior project on this subject came after an elective course we followed during the last term of our senior year. The course was called Cryptography and was given by Assoc. Prof. Cafer Çalışkan. We became very interested in cryptography during the course of the lectures.

We contemplated about how the project can be designed on a daily basis where cryptography is used to our lives. The size of usage area and the datas created have increased significantly with the advancement of technology. Being able to process on these dimensions is causing to reduce the secrecy. Cryptography is an essential part of security today's information systems. Our idea was to investigate a subject in which security could be combined with cryptography. We focused on the security of sending private and secret photos.

First of all, we would like to thank Assoc. Prof. Cafer Çalışkan who helped us greatly by considering our request while choosing the topic and during the stage of the developments of our project.

TABLE OF CONTENTS

ABSTRACT

Cryptography has always been an important way to protect personal and national security. It is not only takes place in the army but also in civilian areas: with the personal computers of the eighties, cryptography has become available to everyone. Nowadays, an ordinary computer can produce such complex codes that the most powerful supercomputer which uses the most sophisticated attack algorithms will not break them in thousands of years. Cryptography is used to secure phone, internet, email communications to protect the software and the other digital assets. In general: to keep privacy in the bad world of communication, it is possible to communicate without being spied by someone or knowing what they say.

we present a system which enables a user to encrypt and decrypt the picture and being able to transfer the data. To achieve the image, both sender and receiver have to know the key. By implementing key expansion, any type of key can be transformed to blok-size key which is taken and used by encryption and decryption process.

1 INTRODUCTION

Today, with the advancement of technology, the size of usage area and the datas that we create in those areas have increased significantly. Being able to be processing on these dimensions causes to reduce the secrecy.

Cryptology has great significance in terms of security and an essential part of today's information systems.. It is a science that applies complex mathematics and logic to design strong encryption methods. Achieving strong encryption, the hiding of data's meaning, also requires intuitive leaps that allow creative application of known or new methods. So, cryptography is also an art.

Cryptography allows you protect the data securely that shouldn't be accessed by perpetrators and helps to provide accountability, fairness, accuracy, and confidentiality. It can prevent fraud in electronic commerce and assure the validity of financial transactions. It can prove your identity or protect your anonymity. It can keep vandals from altering your Web page and prevent industrial competitors from reading your confidential documents. And in the future, as commerce and communications continue to move to computer networks, cryptography will become more and more vital.

Usage area of this project can vary from military to basic daily texting. Businesses and governments use cryptography to provide strong protection against data thieves and to secure classified information. Also, many individuals are using cryptography to protect the personal informations.

2 BACKGROUND

2.1 Cryptography

Cryptography basically tends to some major issues. The first of these areas is privacy. Information must not be passed on to the unwanted people. The other is integrity. The information sent must be a whole. The science of securing data in both way is called cryptography. In that Project cryptography is used for the protecting data.

2.2 Red-Green-Blue Values (RGB)

The aim of project is encrypt and decrypt photos. Therefore to use crypt methods which occurs mathematical calculations there is need to representation colors with the numbers. Hereby RGB is the most used color representation, especially for 8 bit digital images. The RGB is an additive model where the red, green, and blue colors are combined on different quantities. For each pixel we find Red values, Green values and Blue values into three arrays. So we can represent the pixels of an image in the RGB model. This model is so useful for pictures, videos and also using for representing colors in electronic devices.

2.3 Advanced Encryption Standard (AES)

It is one of the cryptography methods. It provides more secure. The Advanced Encryption Standard is used in order to protect data against unofficial access and to encrypt this. The cryptographic process key of varying lengths is used for this purpose. This can be as AES-128, AES-192 or AES-256 depending on the length.

2.4 AES Key Expansion

AES Key Expansion is an algorithm and used to derive the 128-bit round key for each round from the original 128-bit encryption key. This algorithm provides to make AES calculations more secure.

3 CONVENTIONAL CRYPTOSYSTEM

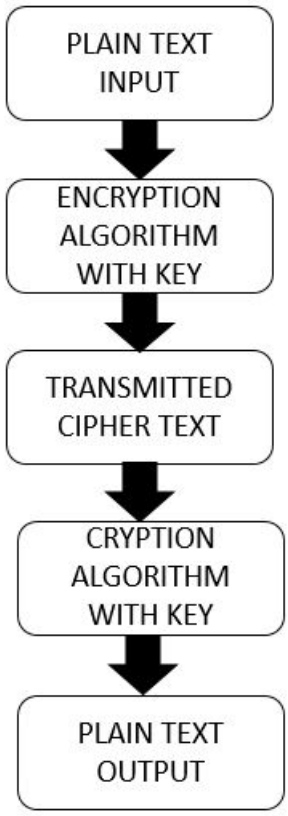

Figure 1 - A block diagram

A cryptosystem is shown in Figure 1 and also has a 5 components:

- Plain text: Plaintext is a term used in cryptography that refers to a message before encryption or after decryption.
- Encryption Algorithm: Encryption algorithm is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. And also, encryption algorithm is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.
- Secret key: Secret key is the part of information or parameter that is used to encrypt and decrypt messages in a symmetric.
- Cipher text: Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.
- Decryption algorithm: Decryption is called decryption of encrypted data into its original format. This is usually a reverse encryption process. Decryption algorithm requires a secret key or password, because an authorized user can decrypt the data.

3.1 The Advance Encryption Standard (AES) Algorithm

3.1.1 Introduction

The more popular and widely accepted symmetric encryption algorithm is currently the Advanced Encryption Standard (AES). The AES algorithm uses a single key for both sender and receiver encryption and decryption. In addition to hardware and software, it is aimed to be implemented in restricted environments and to make good defense against various attack techniques.

3.1.2 Features of AES algorithm

- The data block length can be fixed at 128 bits, and the length can be 128,192 or 256 bits.
- Stronger and faster than DES Algorithm
- It is not a Feistel cipher and works in parallel over the whole input block.
- Designed to be efficient in hardware and software on a variety of platforms.
- It has a total number of rounds is 10,12,14 and key length is 128,192 or 256.
- The 128-bit data block which is divided into 16 bytes, are mapped to a 4x4 array.

- Each round is a uniform and parallel combination of 4 steps such as sub bytes, shift rows, mix columns and add round key.

Version of the AES	Key Length	Block Size	Number of Rounds
AES -128	4	4	10
AES -192	6	4	12
AES -256	8	4	14

Table 1 - Variation of AES

3.1.3 How AES works

Symmetric algorithm use the same key to encrypt and decrypt, so the sender and receiver must know and use the same secret key. All key lengths are considered sufficient to maintain secret informations. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Round conversion, transparency, and input consist of various processing steps, mixing plain text and converting it to the final output of the cipher text. We have used AES-128 bit algorithm in our project.

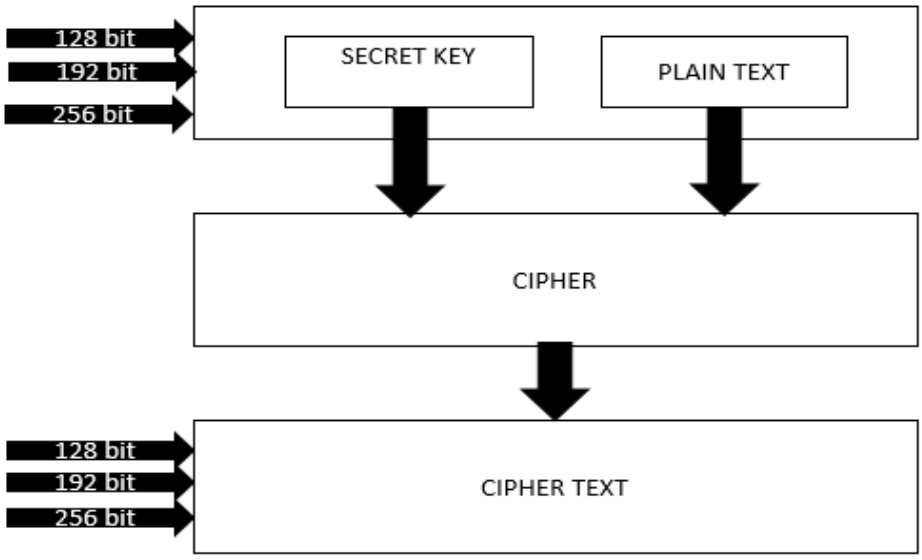

Figure 2 - Explanation of AES

4 IMPLEMENTION OF AES-128 BIT ALGORITM

4.1 Encryption

High-level description of the algorithm

1. Key Expansions round keys are generated from the cipher key using the key Rijndael's key schedule. A separate 128-bit round key block for each round is required by AES and plus one more.

2. Initial round

   AddRoundKey Involves bit-wise XOR operation. By using bitwise XOR, each byte of the state is combined with a block of the round key.

3. Next rounds

   - SubBytes: Operates each byte of the State independently. A non-linear substitution step where each byte is replaced with another according to S-box. Each byte is substituted by corresponding byte in the table.

   - ShiftRow: Cyclically shifts the rows of the State over different offsets. A transposition step where the last three rows of the state are shifted periodically at regular intervals.

   - MixColumn: In this operation the column of the State are considered as polynomials over GF(2^8) and are multiplied with a fixed polynomial. The MixColumn component does not operate in the last round of the algorithm.

   - AddRoundKey

4. Final round

   1. SubBytes
   2. ShiftRows
   3. AddRoundKey

4.1.1 Key Expansion

Key Expansion:

To create round keys for each round, AES uses a key expansion process. If the number of rounds is N , the key-expansion routine creates N+1, 128-bit round keys from one single 128-bit cipher key.

In a simple cipher, it can be XOR the key with the plaintext. Such a step is easily reversed by another XOR from the same key as the encrypted text. In AES, there are numbers of rounds, each of needs its own key, so the actual key is “stretched out" and converted to give key segments for each round. This partition is the key expansion. As part of the generic AES algorithm, the key expansion routine takes an input key. The output is an expanded key.

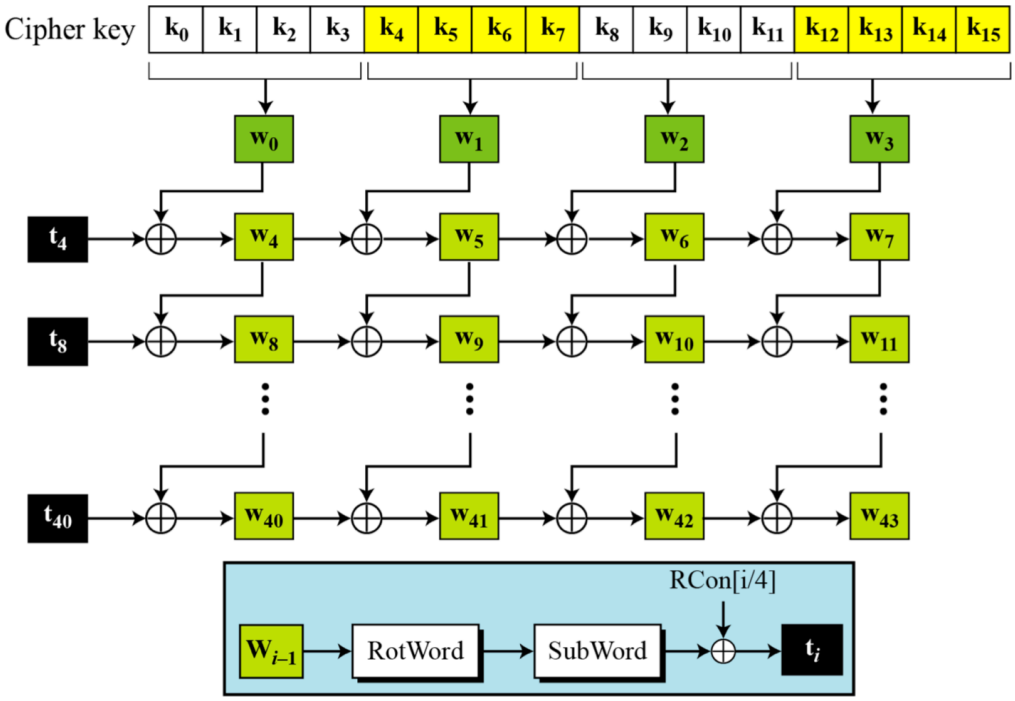

Figure 3 - Key Expansion in AES

4.1.2 SubbBytes

In the SubBytes step, each byte in the matrix is updated by using 8-bit substitution box which is called as Rijndael S-box. This process is providing the non-linearity for the encryption. S-box used is derived from the multiplicative inverse over GF(2^8) that is well

known non-linearity properties. The S-box is structured with the combine of inverse function with an invertible affine transformation to avoid attacks which is based on simple algebraic properties. The S-box is also used to avoid any fixed or opposite fixed points. In the decryption process, the inverse of Subbytes is used, which requires first taking the inverse of the affine transformation and then finding the multiplicative inverse.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 4 - S-Box Table

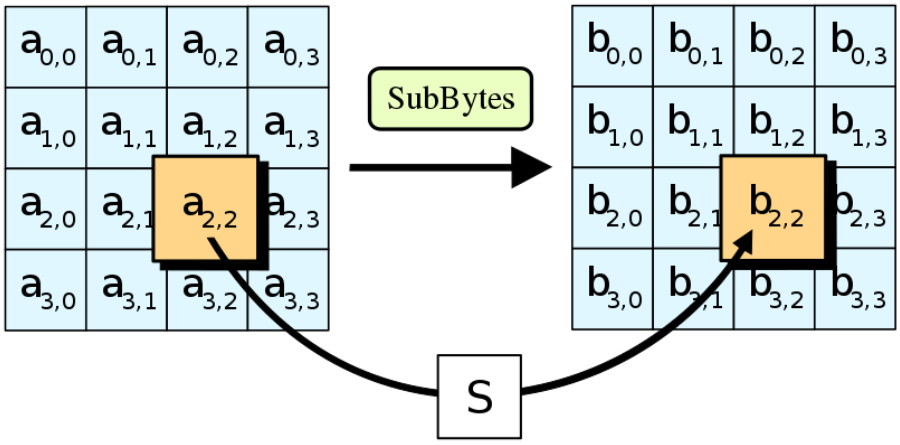

Figure 5 - In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table.

4.1.3 Shift Rows

After the Subbytes step, The ShiftRows step operates on the rows, it cyclically shifts the bytes in each row with the certain offset. In AES encryption, the first row is not changed. In the second row, each byte is shifted one to the left. Likewise, the third and fourth rows are shifted in order of by offsets two and three. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row *n* is shifted left circular by *n-1* bytes. In this way, each column of the output state of the ShiftRows step consists of the bytes in the input state. (Rijndael versions with a larger block size have slightly different offsets). The priority of this step is to avoid from independently encoded columns; in this case the AES will be transformed into four independent block ciphers.

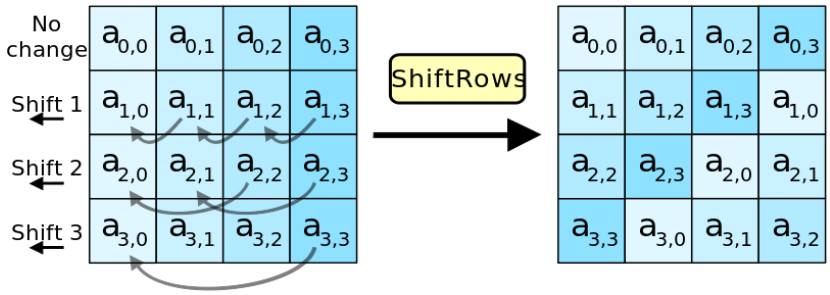

Figure 6 - In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

4.1.4 Mix Columns

In the MixColumns step, four bytes of each column are combined using a recursive linear transformation. The MixColumns function takes 4 bytes of input and 4 bytes each, which affects the four output bytes of each byte. Along with ShiftRows, MixColumns provides diffusion in the code. During this operation, each column is transformed using a fixed matrix (matrix left-multiplied by column gives new value of column in the state):

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Figure 7 - Mix Column Table

Matrix multiplication is composed of multiplication and addition of the entries. Entries are 8-bit bytes treated as coefficients of polynomial of order x^7. Addition is simply XOR operation. Modulo irreducible polinomial of multiplication is $x^8+x^4+x^3+x+1$.

If process is occurred bit by bit, then, after shifting, a conditional XOR with $1B_{16}$ should be performed if the shifted value is larger than FF_{16} (overflow must be corrected by subtraction of generating polynomial). These are special cases of the usual multiplication in GF(2^8).

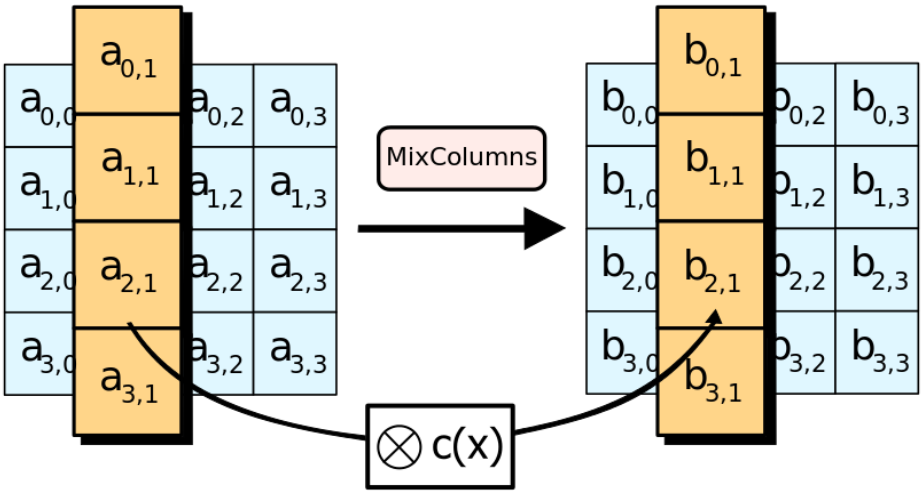

Figure 8 - In the MixColumns step, each column of the state is multiplied with a fixed polynomial c(x).

4.1.5 Add Round Key

The state and the subway are combined in the AddRoundKey step. In each round, the subway is created from the main key by using Rijndael's key schedule. Each subkey has same size with the state. Then the subkey is added to combine each byte of the state with corresponding byte of subkey using bitwise XOR.

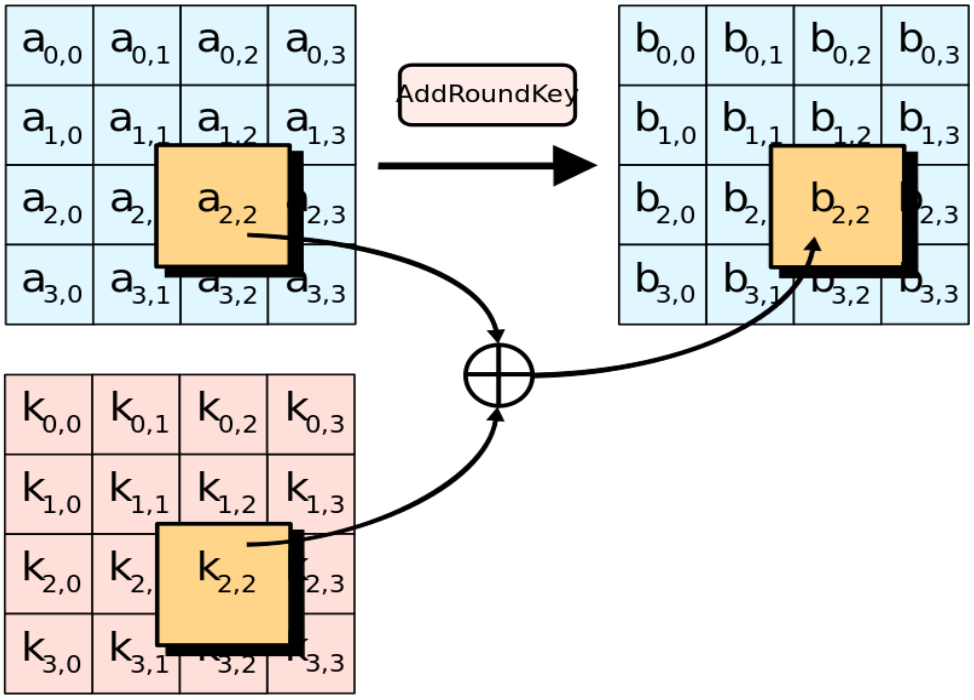

Figure 9 - In the AddRoundKey step, each byte of the state is combined with a byte of the round sub-key using the XOR operation.

4.2 Decryption

In decryption process, Key Expansion and Add Round Key works as they were in encryption part. Key expansion get the key and exchange it according to the blok sizes. Thereafter, in the Add round key step, renewed key is taken and placed on the blocks neatly. The remaining steps' working principles are given at the following.

4.2.1 Inverse Shift Row

Inverse Shift Rows step is the inverse of the Shift Rows step which occurs in encryption process. The bytes in the last three rows of state are cyclically shifted to bytes in different numbers. The first row is not shifted. The rest of the rows are cyclically shifted with the value of left shift depending on row number.

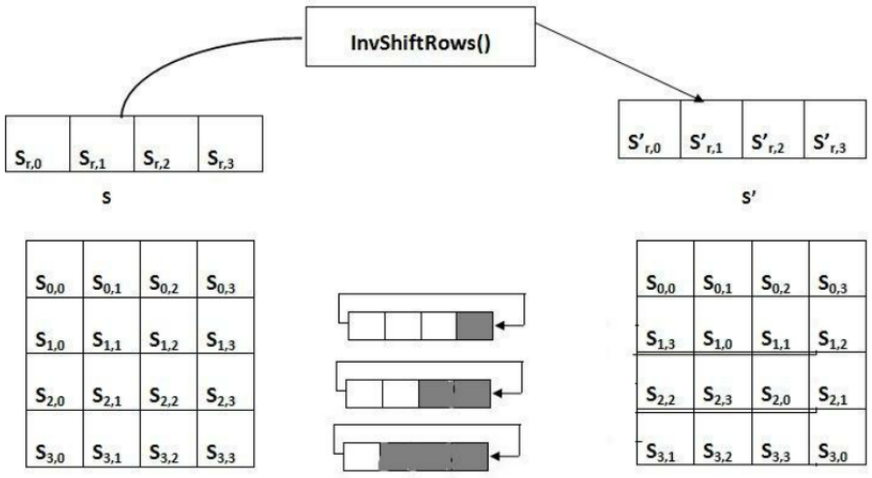

Figure 10 - Inverse Shift Row Pictorial Representation

4.2.2 Inverse Substitute Byte

Inverse Substitute Bytes is the inverse of the SubbBytes transformation which is held in encryption process. In this state, the inverse S-box is applied to each byte. This is achieved by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF(2^8). There is an inverted s-box table to substitute the values.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure 11 - Inverse S-Box

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \text{Inverse} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

C $\qquad$ C^{-1}

Figure 12 - Tables of MixColumn and Inverse of MixColumn

4.2.3 Inverse MixColumns

Inverse Mix Columns is the inverse of the Mix Columns transformation. Inverse Mix Columns operates on the State column by column, that treat each column as a four-way polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial (x), given by

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

5 CRYPTOGRAPHIC PICTURE ENCRYPTION TECHNIQUE BASED ON THE RGB PIXEL

5.1 Introduction

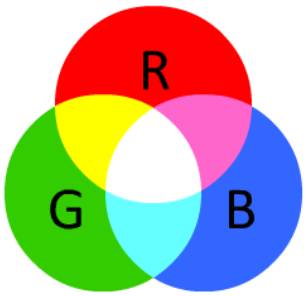

Figure 13 - Visualization of RGB Values

In cryptography, encryption is the process of converting information by using an algorithm to make it unreadable by anyone except those with special features. The information, usually referred to as the key, is encrypted as a result of the operation.

Cryptography in digital computing has also been applied to file formats such as text, pictures. In this report, an image-based encryption technique is proposed by mixing an RGB pixel value and developing an encryption algorithm for m * n-dimensional image encryption. The algorithm makes it possible to encrypt and decryption images by RGB pixel.

RGB is the most used color spaces, specially for 8 bit digital images. The RGB is an additive model where the red, green, and blue colours are combined on different quantities. Representing the pixels of an image in the RGB model. The pixels of an image represented in the RGB model have usually 8 bits depth, resulting in 256 possible. It means for green 256, for red 256 and for blue 256 different tone we would have. Then total tone scale will be very large. So this model is so useful for pictures, videos and also using for representing colours in electronic devices.

For our Project that model is important. Because the aim is using each specific pixel's mathematical representation (digital image) which are the RGB number and coordinates to crypt the each pixel.

5.2 Result of working process in RGB

The images are divided into pixels. Red, green and blue values of the images are taken and created the lists according to pixel numbers. This valued list is divided into 16 blocks. Each encrypt algorithm is applied. If the pixel number of the picture is not a multiple of 16, padding could be done. However, the security level of the system will decrease. This situation causes the system to become known. The values to be taken to the blocks are returned to the per-image each time. Then, encrypted numbers which in form of hexadecimal are converted to decimal numbers. With the "set image" class that we generated in java code, we created a new image by entering the each pixels' values.

Figure 14 - RGB values and pixel numbers in our project

6 DESIGN OF THE PROJECT

In our Project we used Java for the implementations. Because Java is the most common used programming language for mobile applications and for the other applications. For the design part Eclipse and IntelliJ provides Swing library to make form applications. This is more efficient than creating with coding.

The application is taking photo from browser and encrypt the photo with AES. There is a frame to show chosen photo and another place to show encrypted or decrypted image. In addition, we added a Paint property to our application. By clicking to edit button the user can write something or drawing shape on the photo and then can encrypt it. After saving the encrypted photo, user can send it to the target.

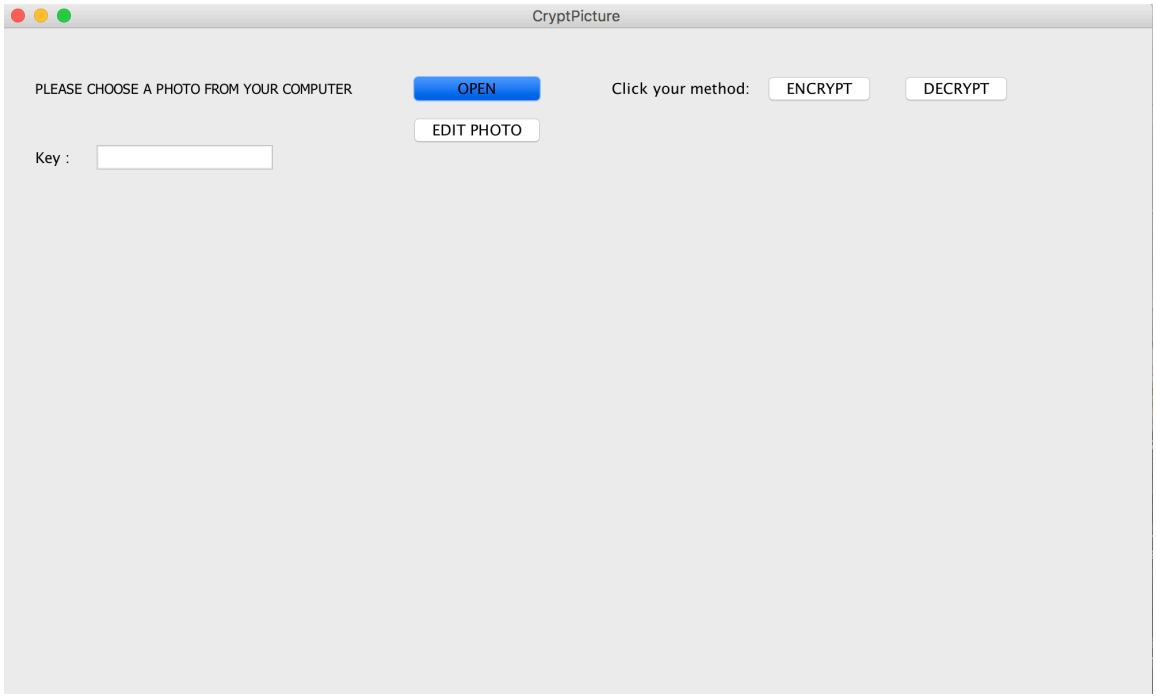

Figure 15 - Fresh looking of the app when it is opened

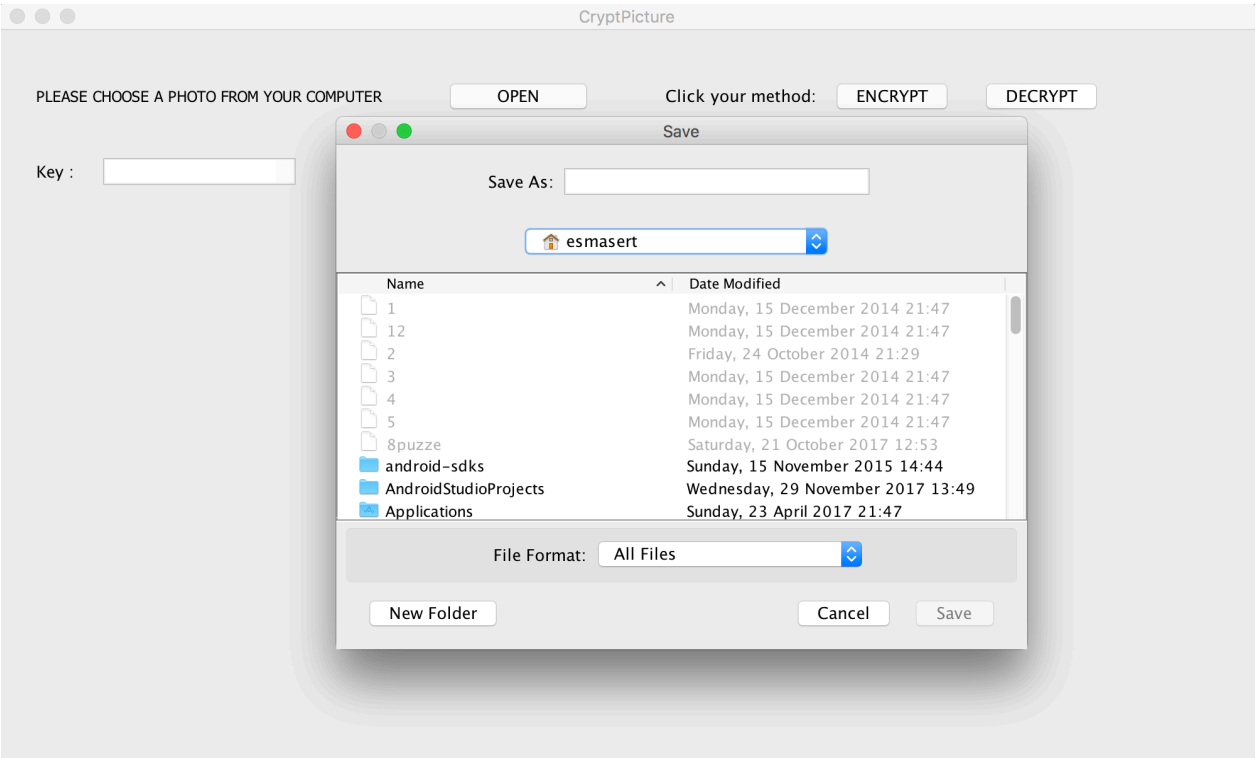

Figure 16 - Selecting the target image

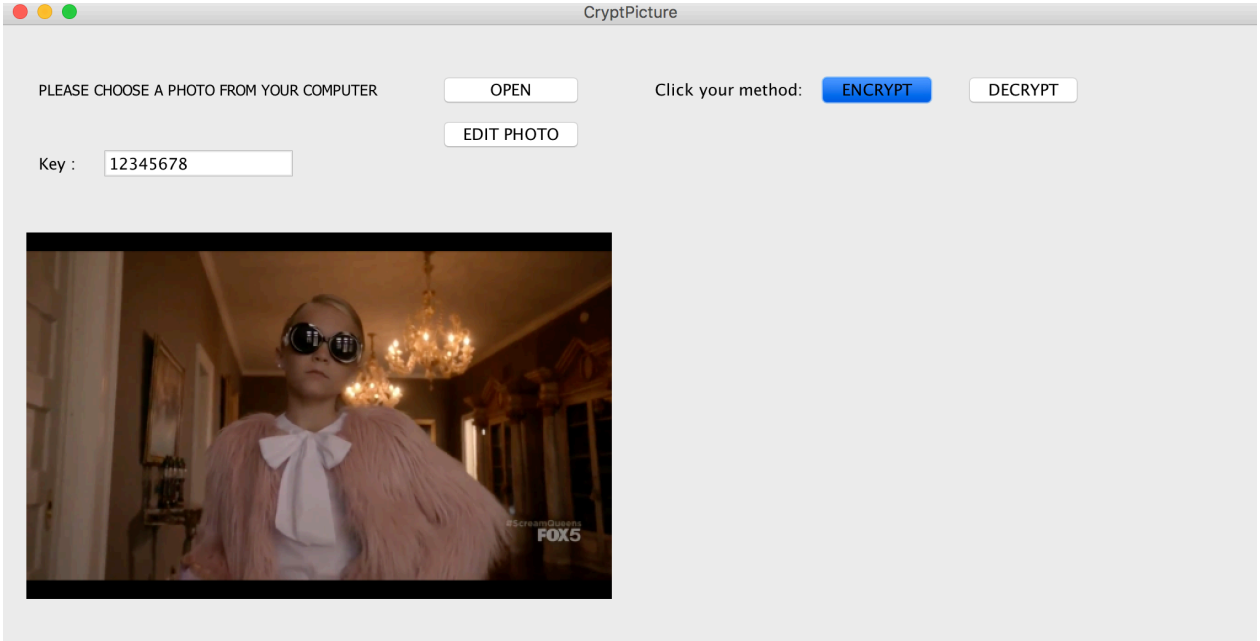

Figure 17 - Selected image is opened

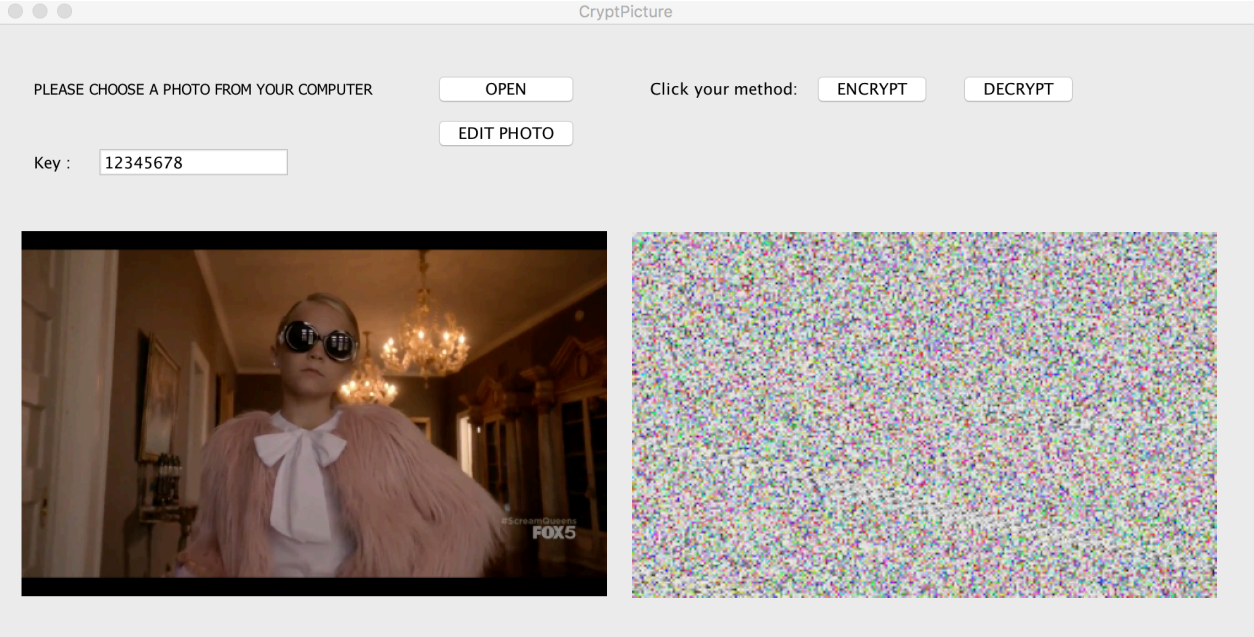

Figure 18 - Selected Image is Encrypted.

7 RESULT

Encrypted images will be obtained and these files can be sent to the target or just remain on the computer. In the same way, the original image can be obtained by decrypting the encrypted image which is sent by target. In addition, our project can be combined with the other projects. For instance, the images is taken by drones which is used for military areas can be delivered in a secure way. There is another feature, the original photo can be edited as writing some notes on it or indicating a point in the picture.

7.1 Potential Progress of the Project

7.1.1 Drones

Drones, which are also called unmanned aerial vehicles (UAVs), does not have a human pilot and is instead controlled by a person on the ground or autonomously controlled by a computer program. This craft is becoming increasingly popular not only

for war and military purposes, but also for disaster relief and sports photography from wildlife and atmospheric research.

Our project is adaptable to the drones. During the video shoot of the Drones, fast photographs are taken that will not be perceived by the human eye and those photos are sent to the target side and look like a video to the human eye. By encrypting these images one by one, it seems like encrypting the video and so the security can be improved in the military field.

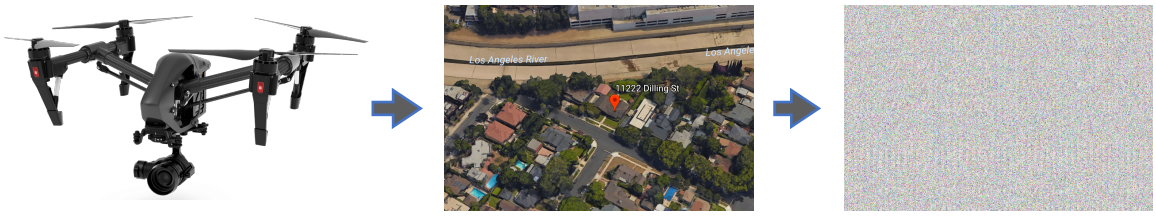

Figure 19 - Usage of Program With Drone

7.1.2 Data Compression Implementation

Our project will use mostly high-quality photographs. Sending these type of photos over the network or internet takes a lot of time and space of memory. Therefore, we are planning to implement data compression to prevent those wastage of time and memory.

Data Compression changes the structures of the data so that it occupies less memory. In short, this is the process of encoding or transforming. It allows to reduce the storage size of one or more data. It also allows data objects and files to be sent quickly over a network or internet.

Data compression has wide implementation in computing services and solutions, specifically data communications. Data compression works through several compressing techniques and software solutions that utilize the data compression algorithms to reduce data size. It removes and replaces the repetitive data. Therefore, data compression for graphical data can be non- missing compression or lossy compression, where the former saves all replaces and repetitive data and then deletes all the repetitive data.

7.1.3 Error Correction Implementation:

Error correction which is reconstructing the original error-free data, is the process of detecting errors. In addition, error correction makes sure that corrected messages and error-free messages send to receivers.

Our project will be a comprehensive field.It will be used for transfer of information that is of greatest importance when needed.Therefore, in case of adverse situation to be met in any case, it is necessary to protect original information of all information.In this case "error correction" will be provided.For example, When data is transferring to target place, if weather condition is not good enough data can get damaged.

7.1.4 Messaging Application

The program can be developed and converted into a messaging application or mail program. Thence high security communication can be provided which can send messages and cryptographic pictures to each other on both sides. While this may be something that everyone can use in daily life; also, it can be used for mailing among the companies if an appropriate application is made to it. Mobile applications and desktop applications that are in the upper level of security can be designed and produced.

8 CONCLUSION

In conclusion, information security has decreased day by day by the enhancing of usage of the technology. Cryptology has been tried to protect the security while communication is occurred. Encryption in cryptography is the conversion of information by using an algorithm to make it unreadable by anyone except those who have the private information, with the accessing of the key. Therefore, it will ensure the data security of the data. we have worked on the security of our photo transmission in our project. We worked on sending the photos in a secure way to provide the security of communication. Our project is using pixels and it’s red, green, blue values, we are using AES encryption method to encrypt the images. We also provided decryption to find the original photo from the encrypted picture. Besides, our project provides transferring the chosen image without losing any data.

9 REFERENCES

Anuja P. Parameshwaran, Wen-Zhan Song, 2016, *Encryption Algorithm for Color Images: A Brief Review of Recent Trend.*

Christof Paar, Jan Pelzl, 2009, *Understanding Cryptography*.

N.K.Pareek, Vinod Patidar, K.K.Sub, 2006, *Image Encryption using chaotic logistic map*.

Priya Deshmukh, 2016, International Journal of Scientific & Engineering Research, *An image encryption and decryption using AES algorithm*, Vol. 7, Issue 2, ISSN 2229-5518.

P. Kartigaikumar, Soumiya Rasheed, 2011, *Simulation of Image Encryption using AES Algorithm.*

Quist-Aphetsi Kester, 2013, *Image Encryption based on RGB PIXEL Transposition and Shuffling.*