IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 11, November. 2019, Series -III, PP 06-08

AES and Color Coded Cryptography

Reena Manjrekar[1], Sanika Rathod[2], Ankita Thamke[3]
Student Department of Computer Engg, Vidyalankar Institute Mumbai, India.
Corresponding Author: Reena Manjrekar
Received 08 November 2019; Accepted 25 November 2019

Abstract: In our encryption mechanism, the Plaintext is converted into color coded pixels. The output for certain given input (.txt file/string) is a bitmap image and the
companion file without which the file won't decrypt (this is also encrypted in AES for security purpose), the user has to provide password during the encryption phase.
The same password is required to decrypt the file. Example: - during the decryption phase all the three viz; image, companion file and password is required if any given value is wrong i.e. the file or password for the given bitmap image will result in an error. This way it makes it difficult for cryptanalyst to analyse the output (the image to gain the information which was present in the actual file). In the case if the user wishes to encrypt any other format file s/he can use "Encrypt with AES" Function of our software and can be decrypted only with the "Decrypt with AES"

Keywords: Advanced Encryption Standard (AES), Colour Coded Cryptography.

I. INTRODUCTION

Information Security which refers to protecting information in potentially hostile environments is a crucial factor in the growth of information-based processes in industry, business, and administration. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society.

The security of cipher text is completely dependent on two things: the power of the cryptographic algorithm and the confidentiality of the key. Intruder activities in recent times have created a need for inventing stronger and more secure algorithms. In recent past many researchers have modified the existing algorithms to fulfil the need in the current market, yet the ciphers are vulnerable to attacks.

The emerging threats to information security are increasing at an alarming rate. Any information stored on a computer/server connected to a network (internet/intranet) has 99% Chances of getting leaked. The most influential and universal approach to counter such threats is encryption. Traditional encryption techniques use substitution and transposition.

Substitution techniques map plain text into cipher text. In all traditional substitution technique characters, numbers and special symbols are substituted with other characters, number and special symbols. (In the case of substitution, if the characters in Plain Text are repeated, then, corresponding characters in Cipher Text are also repeated).

II. LITERATURE SURVEY

Sr. No	Title, Author name and year	Description
1.	Text encryption using colour substitution and AES • Amal Joshy	**Algorithm:** Colour coded and AES text
2.	Cryptography based on colour substitution • Vishaka Nayak	**Algorithm:** Colour coded encoding text

PROPOSED SYSTEM

Proposed System is a Desktop application that lets the user encrypt and decrypt data using colour coded mechanism / AES256 depending on the file type. For a
.txt file or a string the software will use Colour Coded Mechanism for encryption and in case of any other file format AES 256 is used.
eg:

- **For Colour Coded Mechanism**
- User makes a file using our software (instead of using MS-word) and the output is a image file(bitmap image) and a AES256 encrypted companion file(key without which the file won't be decrypted) the user will add a password as well(Defence in depth mechanism).
- To decrypt the "cipher text" (image in our case) the user will require to use our software, the companion key file and the password used while encrypting without which the file won't be decrypted.

Entering wrong password more than **3** times will result in destruction of the file (that would provide a protective layer from **brute force attack**)

- **AES 256**
- The user selects a file and enters a password and the user is give an encrypted file
- The user selects the encrypted file and the password which gives him/her the decrypted file

Encryption Mechanism

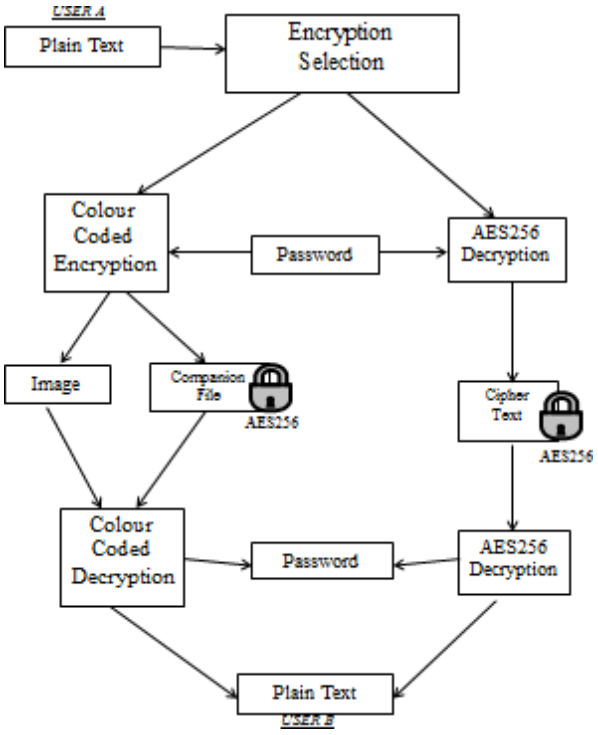
- A random 6-digit key is generated
- Each character from the Message (text) is converted into ascii **ch** and passed into a function say **encrypt () and** the character position **pch** is passed as well.

Encrypt (): now the ascii value, block size n, key, character position is passed in this function. In this function RGB channels are choosed.

After the Encrypt () is executed the output of this file will be a cipher text(bitmapping), and a companon file (encrypted with AES 256).

Decryption Mechanism

- At the receiver side the receiver inputs the cipher text (bitmap img), key and the password
- The password is then used to Decrypt the companion file first.
- **Decrypt ():** For every n blocks the value of pixel is checked and depending on the chosen channel for transmission of data the other two values are ignored. Once the decrypt () function is executed the value of ch at position pch



III. FUTURE SCOPE

This project has various advantages due to which it has a very good scope the following are the features:

- Cryptanalysis would require to analyse the whole image which would require extensive forensic knowledge
- This is completely different than image steganography (hiding data inside an image) as here the "image is the data"
- As mentioned earlier the password counter mechanism will provide protection against brute-force attack that could be used to crack the password.
- Without all three (image, companion file(key), and password) it is virtually impossible to decrypt the file.

IV. CONCLUSION

- Encryption using Colour Coded Mechanism will make it hard for cryptanalysts/hackers to get hands on to the ciphertext without authorization
- AES 256 is used to Encrypt all other file formats and the companion file which makes it a lot more secure compared to its counterparts
- Decryption for files encrypted with colour coded mechanisms require the user to enter password, the companion file and the bmp image(cyper text) without which the file wont be decrypted which adds an extra layer of Security

REFERENCES

[1]. https:// HYPERLINK"https://www.dyclassroom.com/image-processing-project/how-to-create-a- random-pixel-image-in- java"www.dyclassroom.com/image-processing-project/how-to-create-a- random-pixel-image-in-java
[2]. IEEE paper on text to image encryption
[3]. https://HYPERLINK"https://www.dyclassroom.com/image-processing-project/how-to-get-and-set- pixel-value-in- java"www.dyclassroom.com/image- processing-project/how-to-get-and-set- pixel-value-in-java

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Reena Manjrekar. "AES and Color Coded Cryptography." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 11, 2019, pp. 06-08.