Secure Approach Using Visual Cryptography

(Karan Gupta, Deepanshu Kumar Singh, Abhishek Kumar Pal, Animesh Pratap Singh)

UG student of Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, Uttar Pradesh, India

(Er. Ankit Khare, Dr. Ashish Baiswar)
Assistant Professor, Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, Uttar Pradesh, India

ABSTRACT: An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm is proposed in this paper. Visual cryptography is the most popular technique attracted various researchers to improve the security level while utilizing the images and videos as encryption key, instead of text which is easy to crack. **Visual cryptography computes complex multimedia information which may leads to computational overhead when simple processing techniques and architectures were utilized. So, various researchers had taken over this challenge and trying to resolve while introducing the various high speed techniques and architectures which would make visual cryptography process highly secured and energy efficient. This paper presents an algorithm in which the image is an input to AES Encryption to get the encrypted image and the encrypted image is the input to AES Decryption to get the original image.**

Keywords*:* Visual cryptography, security, energy efficient, high speed architecture, accurate prediction outcome, AES algorithm, image encryption, image decryption

I.INTRODUCTION

Visual cryptography is the process of encrypting the multimedia contents such as images, videos and audios etc. Visual cryptography appears to be more complex task where the visual data needs to be encrypted without losing the original visual content information. In recent world, various research applications such as data security, data hiding would requires to handle visual information for the improved performance. Most of the organization started to concentrate on data security and hiding techniques due to increased usage of computer generation. To achieve this organizations spend millions of amount, thus the security of their industries can be ensures. This is done due to increased threaten towards cyber theft and crime. Increased technologies made easier environment for the criminals to involve in the Cyber Crime activities with partial known information about the industrialists. These issues can be resolved by introducing the cryptography techniques. Particularly visual cryptography plays major part in the increased security level due to its complexity level. Encryption process involved in the visual cryptography technique increased its applicability and usage in various. Symmetric systems contains Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) uses an identical key for the sender and receiver. DES (Data Encryption Standard) was considered as the standard of symmetric key encryption, which has a key length of 56 bit. This key length is considered as very small and can be easily broken. The National Institute of Standards and Technology (NIST), proposed Rijndael algorithm as the Advanced Encryption Standard (AES) in October 2000 providing strong security and high flexibility. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

2.PREVIOUSWORK

In paper Mazen El Maraghy Used AES-128 bit algorithm for optimization of area and speed. They have used128 data bits as well as 128 bit cipher key. The implemented hardware design is evaluated in real time. M.Sambasiva Reddy used the same AES-128 bit algorithm for speed, power consumption and area. They have implemented the AES algorithm using EDK. Hoang Trang This gives low complexity architecture and easily achieves low latency as well as high throughput. The design used an iterative looping approach with block and key size of 128 bit, lookup table implementation of S-box. Kamali S.H used the modified advanced encryption algorithm to reflect a high level security and better image encryption. The modification is done by adjusting the Shift Row Transformation. The author have compared the results of the previous AES algorithm and modified AES algorithm.

AES has four main operational blocks:

1. Substitute byte transformation: An S-box is used to substitute each data block byte with another block.

2. Shift transformation of rows: Each row of the state matrix is given a cyclic shift to the right side according to its location.

3. Mix Transformation of Columns: It is a matrix multiplication operation where each column of the state matrix is multiplied by that of the fixed matrix.

4. Add Round Key Transformation: XOR operation is performed between the new state matrix and the round key one.

3.PROPOSED WORK

Three important factors must be considered for designing an algorithm:
The algorithm must be simple enough to be evaluated and analyzed easily and completely.
An encryptor must provide security margin more than the required value against the known attacks.
Well-known, well-examined and reliable instruments and ideas must be used for the design.

According to the above-mentioned points, using the combination of modified AES algorithm, an image encryption algorithm is proposed here which is an efficient one from both security and speed aspects. This paper uses the overall structure of the standard AES algorithm. Some modifications have been made to make the proposed method suitable for the image encryption.

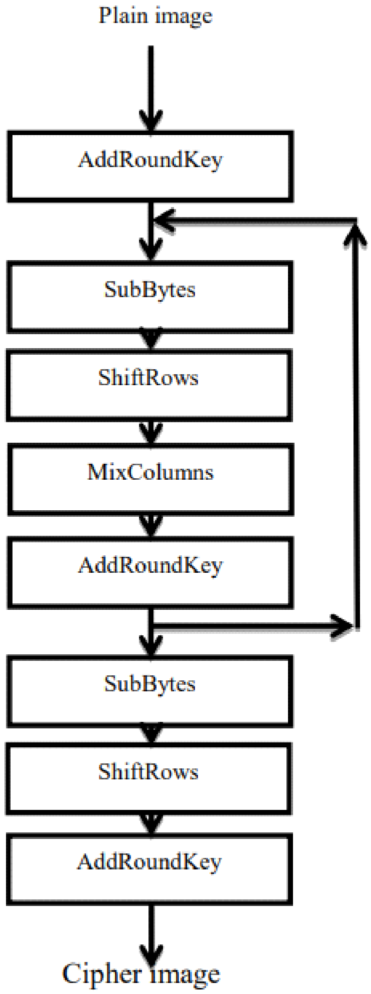


Figure 1: AES Image Encryption

3.1 AES Algorithm

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed system consists of block size of 128 bits and key size of 256 bits. The algorithm is applied for both image encryption and decryption. As the key size is of 256 bits it will take 14 rounds

.

3.1.1 AES Image Encryption

Conversion of original image i.e plain image into encrypted image i.e cipher image is known as image encryption. The round consists of the following stages for image encryption

□SubstituteBytes

□ShiftRow

□InverseShiftRow

□AddRoundKey

SubstituteBytes:

The SubBytes transformation includes non-linear byte substitution, operating on each of the state bytes independently. This is done by using a once-precalculated substitution table called S-box. S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values.

ShiftRow:

ShiftRows transformation includes, the rows of the state are cyclically left shifted. Row 0 remain unchange; row 1 does shift of one byte to the left; row 2 does shift of two bytes to the left and row 3 does shift of three bytes to the left.

InverseShiftRow:

InvShiftRows exactly functions the same as ShiftRows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.

AddRoundKey:

In the AddRoundKey transformation, a Round Key is added to the State resulted from the operation of the MixColumns transformation by a simple bitwise XOR operation.

3.1.2 AES Image Decryption:

Reverse of encryption is called decryption. It means conversion of cipher image into plain image. The round consists of the following stage for image decryption shown in fig 2.

□ AddRoundKey

□ InverseShiftRow

□ InverseSubstituteByte

□ InverseMixColumns

AddRoundKey:

AddRoundKey is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order.

InverseSubstituteByte:

The InvSubBytes transformation is done using a onceprecalculated substitution table called InvS-box. That InvSbox table contains 256 numbers (from 0 to 255) and their corresponding values.

InverseMixColumns:

In the InvMixColumns transformation, the polynomials of egree less than 4 over GF(28), which coefficients are the elements in the columns of the state, are multiplied modulo (x4 + 1) by a fixed polynomial d(x) = {0B}x3 + {0D}x2 + {09}x + {0E}, where {0B}, {0D}; {09}, {0E} denote hexadecimal values.

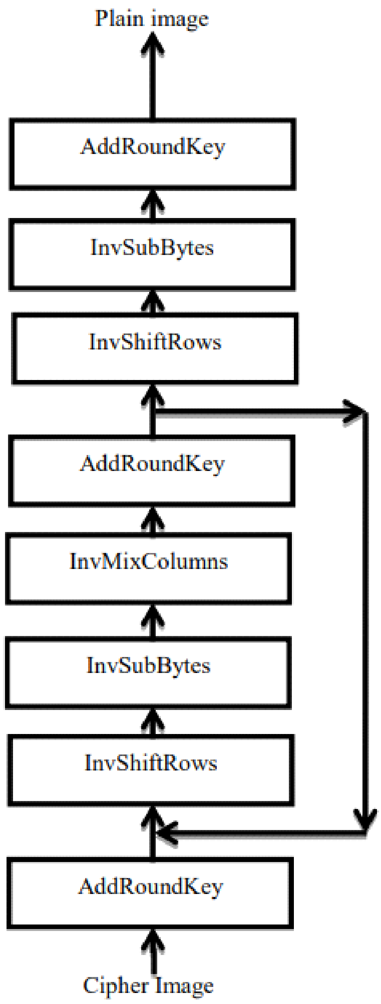


Figure 2 AES Image Decryption

4. NUMERICAL ASPECTS & METHEDOLOGY

AES algorithm consists of the following four base procedures. Sub Bytes Transformation: The SubBytes () transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table. Shift Rows Transformation: In the Shift Rows () transformation, the bytes in the last three rows of the state are cyclically shifted over different number of bytes. The first row will not get shifted. Mix Column Transformation: In Mix Column (), the columns of the state are considered as polynomial and then multiplied by modulo with fixed polynomial, individually. AddRoundKey Transformation: In the AddRoundKey () transformation, a round key is added to a state by a simple bitwise XOR operation. Each round key consists of Nb words from the key schedule; those Nb words are each added into the columns of the state. To encrypt the shares the input is considered as a share. Hence, the shares are taken that is converted into block matrices. During the encryption process, the shares are undergone to the basic procedure of AES algorithm and the output is encrypted share. In this process, shares and AES algorithm binds together to give the resultant shares are called the encapsulated shares.

Input: Encrypt - (I), (K), (N)
Output: (CI), 1, 2… N (KI)
Here I – Image to be encrypted. Supports various standard formats.
K – Key File given as a sequence of characters.
N – Number of shares of Key to be generated (min 2)
CI – The base64 encoding of the encrypted image I.
KI – N images or shares of the Key that are generated

Algorithm (with N = 8):

Step 1. Read the input image and encode it using base64 standard.
Step 2. Read the key file and initiate the AES 256-bit key file.
Step 3. Encrypt the image using the base 64 encoded text and hash generated in steps 1 and 2 respectively.
Step 4. Create a new Image C of size (w, h) with pixel data p where
a. w - character support for key file (Default: 255)
b. h – Number of characters in the key file
c. p – Pixel Data to be filled (Default: 0)
Step 5. For-each row i in height of image repeat:
a. Let j be ASCII code of the ith character in the key file.
b. Fill the first j pixels of the image in the ith row with black color.
i. C [i] [j] = 0 for every i, j in h, w such that j <ASCII(key[i])
Step 6. Create N (= 8) Images (R, P) of the same size (w,h) and pixel data such that
a. For the first image R, pixel data is generated randomly. It can be either 0 (black) or 1 (white). i. R [i] [j] = random (0, 1)
b. Second image pixel data P [i] [j] is defined such that i. P [i] [j] = R [i] [j] xor C [i] [j] for every i, j in (h, w)
Step 7. Output the encrypted encoding CI, Images P and R respectively.

Shares Decryption

The rounds of the decryption algorithm are governed by the following four stages namely the Inverse Shift rows, Inverse Substitute Bytes, Add round key and Inverse Mix columns steps. The inverse AddRoundKey step was eliminated. AES decryption occurs simply as the reverse order of encryption. The encrypted shares are now fed as the input blocks, in which the inverse shifting of the rows value is taken place. It is then followed by the inverse substitution of the pixel positions along with the Key value. Finally, the inverse mix column step was taken place. The resultant image thus produced was the original image at the time of share creation. During the decryption process, the encapsulated shares are extracted by decryption process of AES Algorithm to retrieve the share 1 and share8.

Input: (CI), 1, 2… N (KI)
Output: I Here
CI – Base 64 encoded cipher text.
KI – N shares of the Key that must be supplied for decryption.
I – Decrypted Image

Algorithm (with N = 8):

Step 1. Read the input cipher text of the image CI.
Step 2. Load the Images K1, K2 from the input KI.

Step 3. Create a new Image CK of size (w, h) same as K1, K2 such that
a. CK [i] [j] = K1 [i] [j] xor K2 [i] [j] for every i, j in (h, w)
Step 4. Initialize key K as an array of characters of size same as height of image CK (h).
Step 5. For-each row i in height of image CK repeat:
a. Let count = 0
b. For each pixel j of the image in the ith row with black color.
i. increment count by 1
c. Find the character ki by using ASCII code of the count generated after b. i.e., ki =char (count)
d. Set K[i] = ki
6. With the Key K initialize the AES 256 Algorithm with hash (K)
Step 7. Decrypt the cipher text CI and save the decrypted base64 encoding as an Image I
Step 8. Output the decrypted image I.

Shares Reconstruction Scheme

Figures Finally, all decrypted shares are stacked (Combine these (R1, R2) (G1, G2) and (B1, B2) matrices) together to

retrieve the secret image. Only if all the numbers of secret shared images are stacked together, it is possible to reveal the secrets. If any one of the shares of the original image is missing, it is impossible to retrieve the original image. The

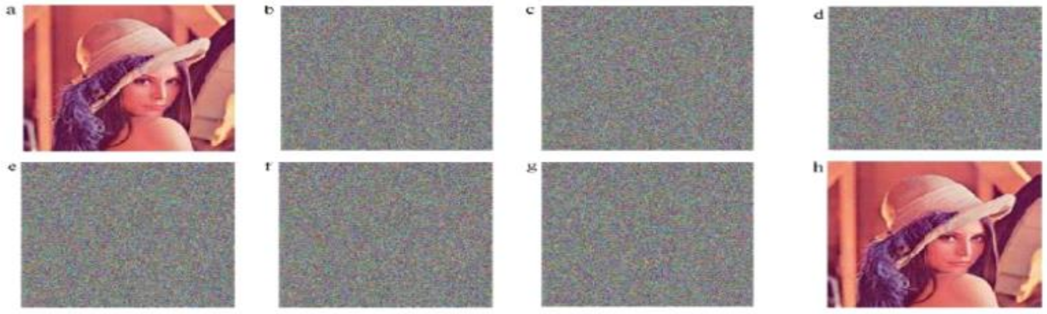
decryption process consists of two steps. First step is done by human visual system where at least k number of shares out of n number of shares is superimposed to give reconstructed image.

I. Input the number shares you have and the same key used for encryption.
II. Shares should be equal to k or greater than k
III. Perform the bitor operation on converted shares to get reconstructed encrypted image.
IV. Now XOR the reconstructed encrypted image and converted key to get 24-bit decrypted image, it then reconstructed to give decrypted image equal to original image.

Human visual system acts as an OR function. For computer generated process, OR function can be used for the case of stacking k number of shares out of n. Second step is decryption of reconstructed image, where pixel array is computed from reconstructed image and XOR with same key used for encryption. Decrypted image is exactly equal to original

image.

FIG 4.1 Reconstruction of image:



5. CONCLUSION & FUTURE SCOPE

In this paper image encryption and decryption using Advanced Encryption Standard (AES) algorithm is proposed for image encryption and decryption that can process with the data block of 128 bit and cipher key length of 256 bit.

The usage of 256 bit cipher key to achieve the high security, because 256 bit cipher key is difficult to break. As a result of this secure transmission of image can be possible. Future scope is, it can be used in various applications like Military communication, Forensics, Intelligent systems etc.

6. REFERENCES

[1] Research paper by 'International engineering journal for research and development Vol.3 Issue 2' proposed by Raj Kamal Gupta, Ankit Sanghavi.

[2] Tutorial point documentations on 'Visual Cryptography' and 'AES methods and approaches formula' Detail understanding on encryption methods etc.

[3] JavaTpoint Documentations on 'Encryption and Decryption' & ' Cryptography' & ' Secure approach of finding the proper crypto methodology' etc.