An Enhanced AES based Secure Image Processing Framework

Bhavana Verma*  
Mtech Scholar, UIET, Kurukshetra University, Kurukshetra, Haryana, India

Sona Malhotra  
Assistant Professor, UIET, Kurukshetra University, Kurukshetra, Haryana, India

DOI: 10.23956/ijarcsse/V7I6/0234

Abstract-In recent years demand of security in image processing is increases because user wants to share images in digital form from one place to another so when an image is transferred between different users than security leakage chances increases. To overcome this kind of challenge number of cryptographic algorithm has been used by different researchers in their work out of them AES is much better and more secure than other algorithms. In this paper we propose an enhanced AES based mechanism for secure transmission of images. We implement proposed mechanism using MATLAB and uses different metrics like histogram and correlation.

Keywords- Image processing, AES, histogram, correlation and Digital image.

I. INTRODUCTION

Image processing is a processing of images in which an image is converted into digital form by using some mathematical operations so that some operations like image enhancing, image extraction and many more can be performed for getting the useful information. In image processing, the input is in the form of video frames, photographs and output is also in the form of image but have some different characteristics. [1] Image processing can be done in analog and digital form or it can be done in two form analog and digital. In analog processing, hard copies are used where various visual techniques can applied so that the analyzer can apply its knowledge and collateral data for processing an image. In Digital form, raw data can processed in computers. For this purpose techniques like preprocessing, enhancement, compression, and extraction can be used. It can be defined as in the form of dimensions like two- dimension. [2]When the matrix is defined in the two dimension, function f(x, y) can be used to represent the function coordinates and the function f represents the amplitude which can be called or named as gray level of image. An image is said to be a digital image when it functions are finite or discrete. A gray scale image can ranges between 0 to 255 with 8 bits representation. An image can be expressed in many formats like: Gif, Jpeg, tiff, etc. [3]

In this paper five sections are presented. In section 1, introduction of image processing has been discussed. In section 2, related work has been presented in which existing techniques for secure image processing has been presented. In section 3, different cryptography algorithm has been discussed. In section 4, Proposed work and in section 5 results has been showed. Conclusion should be described in section 6.

II. RELATED WORK

Li et al. [4] made the underlying endeavor to embrace riotous tent maps (CTM) for picture encryption calculation plan. This framework was simple to the point that its encryption speed is very quick. As a result, it has favorable circumstances in managing expansive number of information and diminishing excess data, contrasted and the regular picture encryption calculations. Be that as it may, some conspicuous deformities can likewise be found in this immaculate CTM-based plan as takes after. In the first place, this cryptosystem just included the diffusing stage, and changed structure has been excluded. Besides, while encoding shading pictures, this plan just scrambles every segment of the shading picture separately, which demonstrates no flexibility from scrambling a dim picture to a shading one.

Zhang et al. [5] researched the security of an exemplary dispersion system (and of its variations) utilized as the center cryptographic primitive in some picture cryptosystems in view of the previously mentioned complex dynamic marvels. Gonçalves and Costa[6] overviewed late advancements in encryption and protection in remote sensor systems sent for transmissions of picture depictions, surveying imaginative ways to deal with give distinctive levels of security. Promising exploration headings were likewise talked about.

Radhadevi and Kalpana [7] displayed a use of AES (Advanced Encryption Standard) operations in picture encryption and decryption. The encoded figure pictures dependably show the consistently appropriated RGB pixels. Proposed approach offers upgraded security, it expects to give client fulfillment by transmitting individual and delicate picture information safely. The Advanced Encryption Standard offers the adaptability of permitting distinctive key sizes 128 piece, 192 piece and 256-piece key and the security depends on the different random key determinations, diverse S-box and solid changes. Padate and Patel [8] depicted an outline of viable security for correspondence by AES calculation for encryption and decryption. It depended on AES Key Expansion in which the encryption procedure was somewhat savvy selective or operation of an arrangement of picture pixels alongside the 128 piece key which changes for each arrangement of pixels. Zeghid et al. [9] adjusted variant of AES, to outline a safe symmetric picture encryption strategy, has been proposed. The AES was stretched out to bolster a key stream generator for picture encryption which can conquer the issue of finished zones existing in other known encryption calculations.
III. COMPARATIVE ANALYSIS

Table 1 Comparative Analysis of Various Cryptography Algorithms

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Development</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES[10]</td>
<td>DES was developed in 1970’s and approved as a weak algorithm in 1977 by NIST (National Institute of Standards and Technology) because of its shortest key length.</td>
<td>It is a symmetric cryptography algorithm which is based on the block cipher mechanism. DES block size is of 64 bits, but only 56 bits are used and rest of the 8 bits are used for the checking of parity i.e., odd parity.</td>
<td>It was a secure algorithm till the 1970’s. It was based on the hardware implementation, hence it runs fast.</td>
<td>It was easily cracked by the Brute Force attack and described as a weak algorithm in terms of security. Its software implementation cannot be described.</td>
</tr>
<tr>
<td>Triple DES[11]</td>
<td>After the Brute force attack DES algorithm was failed in providing security, therefore the Triple DES algorithm was invented in 1998 as a standard ANSI X9.52.</td>
<td>Its block length was of 56, 112, or 168 bits because it encrypts the data three times as in DES and for this it used three keying options, from which keying 1 option is the strongest.</td>
<td>It derived from the DES but simply need to encrypt three times and provides the sub keys and key padding.</td>
<td>It was three times slower than the DES algorithm.</td>
</tr>
<tr>
<td>BLOWFISH[12]</td>
<td>BLOWFISH was designed in 1993 by Brute Schneier in the replacement of DES. It was fast as compared to the DES and Triple DES algorithms and was licensed as free and available for all users.</td>
<td>It has a block size of 32 bits and key size of 32 to 448 bits which is a variable length key size. It has a 16 round Fiestel cipher and resembles CAST-128 which uses S-Box.</td>
<td>It provides more security as compared to the DES. It has a significantly sized key length as compared to the DES.</td>
<td>It cannot be used to encrypt files larger than 4 GB because of its 64 bits block size.</td>
</tr>
<tr>
<td>AES[13]</td>
<td>AES is a first NSA (National Security Agency) was established in 2001 by the U.S. government NIST. Its original name is Rijndael. After approval by the Secretary of Commerce on 26th May 2002, it became effective as federal govt. standard.</td>
<td>Unlike DES, AES does not use Fiestel network, it is based on Rijndael. Rijndael has a key size of 128, 192 or 256 bits and a fixed block size of 128 bits which is larger than the DES block size. It provides the combination of permutation and substitution both. AES implementation can be done in both hardware and software.</td>
<td>It provides the better security as compared to the DES, TDES, IDEA, BLOWFISH, etc. algorithms. It is free of cost. The algorithm provides faster encryption and flexibility as it implemented in both hardware and software.</td>
<td>256 bit keys cannot be used more for encryption because it takes more memory for one round of permutation.</td>
</tr>
</tbody>
</table>

IV. PROPOSED WORK

As the network is growing faster and became bigger, its threats are also increasing day by day. Preventing from these threats some security techniques are required so that data like messages, music, images, etc. can be secured from the unauthorized users, unwanted modification, etc. Security is not only for network security, it is also needed for images like the companies’ blueprints, personal information, medical information, etc. For this purpose various security algorithms like AES, DES, IDEA, Triple DES, etc. are used for encrypting and decrypting the image.

To overcome the drawbacks of above mentioned algorithms, a secure mechanism based on AES is proposed. In the algorithm 64 bits key is used to encrypt the image instead of 128 or 256 bits key. In the existing algorithm, researchers uses 128 bits keys or 256 bits key that uses number of rounds to encrypt the image. Also it takes large amount of processing time and large memory storage which creates overhead.

In the proposed mechanism, only 5 rounds are used to encrypt an image. As described above 64 bits key is used to encrypt an image which is divided into four blocks of 16 bits each.
A. Proposed Framework Description

In this proposed framework, input data is of 64 bits key, which is divided into four blocks of 16 bits each. Then ‘F’ function is applied on the blocks of data and each block is divided into four blocks which carry input data of four bits. These four four bits input data are represented in the matrix form as explained below according to the 128 bits AES algorithms and then X-or operation is applied for generating the keys. These generated keys are used for encrypting the data and for final encrypted key, again X-or operation is applied. The final encrypted key which we get is also 64 bit key.

B. Terms used in Proposed Framework

- ‘F’ Function: The f-function operates on 16-bits data. Therefore four f-function blocks are used. These 16-bits for each f-function are obtained after performing an initial substitution of segments of cipher key. f-function is comprised of A and B tables.
- Key generation process: In each round of process, a different key is to be used. So that an unauthorized person cannot access the personal or secret information from an image. Because of performing less steps or rounds the computation time, memory storage and computation cost should be low.

C. Example for understanding the AES algorithm with 128 bits Key

Let us take an example in which 128 bits AES encryption is applied which using the 10Cycles for the completion of round. It uses a matrix of 4x4 which represents the 16 bytes i.e., 0 to 15. If there are 16 bytes they can be represented in matrix form as $a_0, a_1, a_{15}$.

![Matrix representation](image)

According to the algorithm, each byte is replaced with another byte according to lookup table. It can be shown as:

![Replacing bytes according to lookup table](image)

- Shift Rows step: In shift rows operation, Rows are interchanged with each other. Rows are shifted towards left, for example First row remains unchanged, second shifted by 1 and the nth row is shifted by n-1 bytes.
- **MixColumns step**: In MixColumns, four bytes of columns are combined to make a new column. This can be achieved by multiplying the shift row matrix with the fixed matrix, as shown in the diagram.

![Fig 6: Mixing of columns](image)

- Add each byte to generate the multiple keys.

**D. Flowchart of 64 bit AES Encryption-Decryption Algorithm**

![Flowchart of AES Encryption-Decryption Algorithm](image)
V. RESULTS AND ANALYSIS

MATLAB:
MATLAB is a language which is based on matrix calculations and it is also known as fourth generation programming language. It can be used in the matrix form or in the numerical notations which is used in algorithm development, modelling GUI interfaces. MATLAB is used in image processing, Signal processing and many more applications where mathematical operations like addition, cross product, and Dot products can be performed. In MATLAB various functions like Load, Save Matfile, Disp, Who, Whos, Clear, Clearvars etc. can be used to perform different operations.

Metrics used:
- Histogram: it is used for graphically representation of image cipher values at different intervals.
- Correlation: It is the relationship between two values that how they are dependent on each other. When dependency is low then encryption process is more secure.

Results:
These results are find out with the help of MATLAB where original image is converted into binary form and then it taken as input by scaling the image so that input is of 64 bits key. For encrypted image AES 64 bit encryption algorithm is applied. The original encrypted and decrypted image are showed below with their respective histograms and correlations.

![Fig 8: Encryption Decryption process](image)

In fig 8, Original image is showed at left side in gray color, at center encrypted image and at the right side the decrypted image. The image is decrypted only when correct key will be used for decryption otherwise the image will not be recognized.

![Fig 9: Histogram of original and encrypted image](image)
In fig 9, at the top side original image and at the bottom encrypted image histogram is showed. It shows distribution of intensities after the encryption process. It indicates the level of security. After scaling, the encrypted image histogram shows the smoothing results. The x-axis of the histogram shows the range of pixel values. Since it's an 8 bit image that means it has 256 levels of gray or shades of gray in it. On the other hand, y-axis, shows the count of intensities of image. As you can see from the graph, that most of the bars that have high frequency shows the darker portion of image. That means that the image we have got is darker.

![Histogram](image.png)

In fig 10: Correlation between both images is showed, where left image showed the original image pixels and right image showed the encrypted image pixels. It shows the dissimilarity among original and encrypted data. The original image is highly correlated whereas encrypted image is not highly correlated.

![Correlation](image.png)

**VI. CONCLUSION**

Security of image processing is a challenging task. To protect image from attacker number of existing cryptographic algorithms has been presented in this paper with their pros and cons. After that we provide proposed mechanism which is based on AES algorithm. In this paper we provide 64 bit AES algorithm in which we apply five rounds to generate a secure private key. A secure or more powerful key is not easily attempted by attacker so it increases security. Our results shows that proposed mechanism is more secure because of less dependency between image attributes and more randomness in generation of cipher text. In future we will continue working on it and propose a new mechanism in which less execution time will be consumed with high security in image processing.

**REFERENCES**


