SECURE IMAGE PROCESSING USING AES ALGORITHM

Bhavana Verma[1]

[1]UIET, Kurukshetra University, Kurukshetra,
Haryana, 136119, India
Email-id: [1]bhavana.verma2905@gmail.com

Sonа Malhotra[2]

[2]UIET, Kurukshetra University, Kurukshetra,
Haryana, 136119, India
Email-id: [2] smalhotra2015@kuk.ac.in

Abstract

In today's image communication system security of images is essential. It is necessary to protect confidential image data from unauthorized users. To detect and find unauthorized users is a challenging task. Different researchers proposed different techniques for securing image transmission. In this paper comparative study of these existing techniques has been presented also present types of images and different techniques of image processing with steps used to process an image.

Keywords: Cryptography; Digital image; Advanced Encryption Standard (AES) Encryption and Decryption.

1. Introduction

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. Image processing is a mechanism in which an original image will be converted into digital image and after converting in digital form process it to get useful information. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image [1].In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels [2].

1.1 Purpose of image processing

- Visualization - Observe the objects that are not visible.
- Image sharpening and restoration - To create a better image.
- Image retrieval - Seek for the image of interest.
- Measurement of pattern – Measures various objects in an image.
- Image Recognition – Distinguish the objects in an image [3].

1.2 Types of image processing

The two types of methods used for Image Processing are Analog and Digital Image Processing. Analog or visual techniques of image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing.

Digital Processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction [4].

1.3 Types of Images

The different types of images can be described as follows:

- Binary Images: Binary images represent the binary digit 0 or 1. They are created from the grayscale image by turning value1 i.e., white color and 0 i.e., black color. They are used in Optical Character Recognition (OCR).
- Grayscale Images: Grayscale images are named grayscale because they does not have any color. They create the image color by the grayscale information and contains 8 bits/ pixel data. It is used in medical other fields.
- Color Images: Color Images can be created using three colors RGB i.e.; Red, Green and Blue and can be represented in 24 bits/pixel. However, the actual image is stored in digital image as in the gray- level image.
- Multispectral Images: Multispectral images can be created by using the electromagnetic spectrum bands and are not directly visible to the humans. Examples of these images are X-ray, Radar data, etc. [4].

1.4 Steps of Image Processing

There are the following steps of image processing:

i. **Image Acquisition:** Image Acquisition is the first step of image processing and it also named as digital image acquisition which is used to process an image and this work can be done easily if the image is already in digital form.

ii. **Image Enhancement:** Image Enhancement is the process of improving the quality of image either in contrast or brightness. So, that it is easy for next steps to get the noise free image.

iii. **Image Restoration:** Unlike Image Enhancement, it does not lose the resolution of image during the noise removal process. It can remove the noise from the image and also corrects the blurring image because it works on the scientific point of view.

iv. **Color Image Processing:** It provides hundreds of color in different shades and intensity which can simplify an image in an effective way.

v. **Wavelets and Multiresolution processing:** Wavelets are used to compress an image at different frequencies and using different domains. Multiresolution provides the image in a better quality by increasing its pixels.1

vi. **Compression:** Compression is used to reduce the size of an image, so that it can take less memory in storage and it is mostly used in internet for sending the data.

vii. **Morphological Processing:** It is applied on the binary images to remove or to improve the imperfections in the image. For that Morphological Process uses two basic operations which are Erosion and Dilation. Morphological also uses the structural elements to compare the input of an image with the output pixels of an image.

viii. **Segmentation:** Segmentation is used to get the meaningful image which is very easy to analyze by dividing the image int5o multiple pixels. This can be done either by Thresh holding methods or color based methods, etc.

ix. **Representation and Description:** The output of segment step can be represented and described in the Representation and Description step. As the output of segmentation process in the form of regions and these regions can be represented internally or externally either by pixels or boundaries.

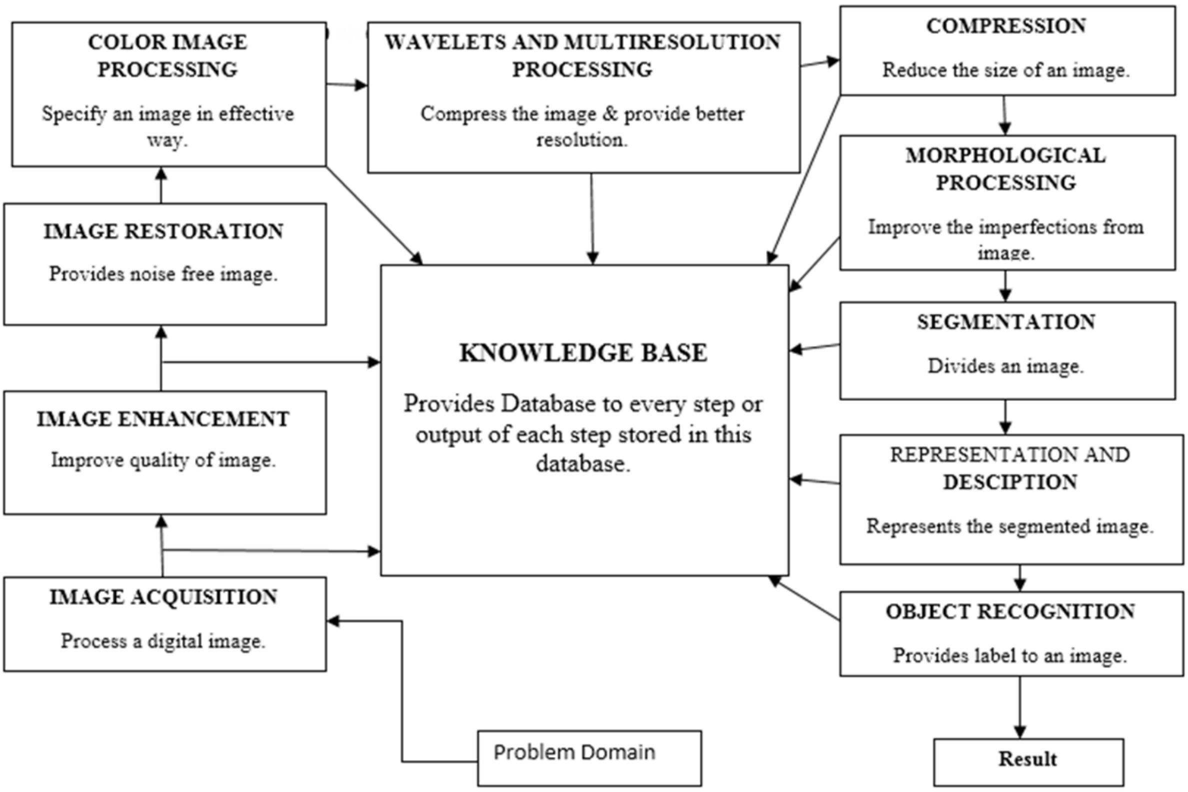
COLOR IMAGE PROCESSING
Specify an image in effective way.
WAVELETS AND MULTIRESOLUTION PROCESSING
Compress the image & provide better resolution.
COMPRESSION
Reduce the size of an image.
MORPHOLOGICAL PROCESSING
Improve the imperfections from image.
IMAGE RESTORATION
Provides noise free image.
KNOWLEDGE BASE
Provides Database to every step or output of each step stored in this database.
SEGMENTATION
Divides an image.
IMAGE ENHANCEMENT
Improve quality of image.
REPRESENTATION AND DESCRIPTION
Represents the segmented image.
IMAGE ACQUISITION
Process a digital image.
OBJECT RECOGNITION
Provides label to an image.
Problem Domain
Result

Figure 1: Steps of image processing

x. **Object Recognition:** When the image is rotated or scaled, it can be recognize at different viewpoints. So, in Object Recognition images can be recognized at various points and we also provides labeling to the images.

xi. **Knowledge Base:** Knowledge Base is the heart of any structure. It provides the database to every step, so it's quite to be complex because every information is stored in that database.[5]

2. Related Work

Security in transmission of computerized pictures has its significance in today's picture interchanges, because of the expanding utilization of pictures in modern process, it is fundamental to shield the private picture information from unapproved get to, Image security has turned into a basic issue. The troubles in guaranteeing people security turn out to be progressively testing. Different techniques have been explored and created to secure information and individual protection. Encryption is likely the clearest one. With a specific end goal to shield significant data from undesirable readers, picture encryption is basic. In these section different techniquesfor image processing to provide secure image processing proposed by various researchers has been reviewed.

Zeghid et al. [6] modified version of AES, to design a secure symmetric image encryption technique, has been proposed.

Upreti et al. [7] proposed an RGB-based, secure technique to maintain and authenticate the integrity of a document.

Fei and cong [8] presented an image encryption algorithm based on 2D Logistic map and complicated Chua's system.

Joshi and Joshi [9] proposed a novel algorithm which comprises of two stages. Henon map was used to encrypt the image and logistic map was used to confuse the image.

Radhadevi and Kalpana [10] presented an application of AES (Advanced Encryption Standard) operations in image encryption and decryption. The encrypted cipher images always display the uniformly distributed RGB pixels.

Padate and Patel [11] described a design of effective security for communication by AES algorithm for encryption and decryption.

Wen et al. [12] proposed a salient region encryption scheme to generate visually meaningful ciphertext. In the proposed method, they extract the salient regions as significant information rather than edge features.

Sekertekin and Atan[13] presented an algorithm for chaotic encryption, which were used Ikeda and Henon chaotic maps.

Goel and Chaudhari [14] proposed a selective encryption technique based on simple mathematics that takes the median of pixel values in a block of image and then calculates percentage deviation of median to decide the pixels that were to be encrypted.

3. Performance Evaluation

In this section comparative analysis of different existing techniques has been presented. There are number of existing techniques available for providing security in image processing system like AES, DES and IDEA. Each technique have its own advantages as well as disadvantages. Table 1 shows description and pros cons of different techniques with their development.

Table 1. Comparative Analysis of various Cryptography Algorithms

Techniques	Development	Description	Advantages	Disadvantages
DES[15]	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.	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.	It was a secure algorithm till the 1970's. It was based on the hardware implementation, hence it runs fast.	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.
Triple DES[16]	After the Brute force attack DES algorithm was failed in providing security, therefore the Triple DES algorithm was invented in 1998 asa standard ANS X9.52.	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.	It derived from the DES but simply need to encrypt three times and provides the sub keys and key padding.	It was three times slower than the DES algorithm.
BLOWFISH[17]	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.	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.	It provides more security as compared to the DES. It has a significantly sized key length as compared to the DES.	It cannot be used to encrypt files larger than 4 GB because of its 64 bits block size.
AES[18]	AEs is a first NSA (National Security Agency) was established in 2001 by the U.S. government NIST. Its original name is Rijndael. After	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	It provides the better security as compared to the DES, TDES, IDEA, BLOWFISH, etc. algorithms. It is free of cost. The algorithm	256 bit keys cannot be used more for encryption because it takes more memory for one round of permutation.

	approval by the Secretary of Commerce on 26th May 2002, it became effective as federal govt. standard.	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.	provides faster encryption and flexibility as it implemented in both hardware and software.	
IDEA[19]	IDEA was designed by James Massey and XerejiaLia in 1991. It was freely available fro non-commercial use. Its patents was expired in 2012 and now it is freely available for all users. Its an open algorithm in PGP standard.	IDEA uses a Lai-Massey scheme which uses a key dependent half round function which works parallel in twice with 16 bits. It operates on a block size of 64 bits and key size of 128 bits which can provide security by is operations deriving from Modula addition, multiplication and XOR.	It provides security against the differential cryptanalysis.	It was broken using a meet in the middle attack in 2011. Two bits reduction in the bits of IDEA can be easily brooked by the Biclique attack.

4. Proposed work

In today's heterogeneous system condition, there is a developing demand for questioned gatherings together to execute appropriated calculations on private information whose mystery should have been protected. Information Security is essential worry for each correspondence framework. The persistent development of Internet and correspondence advancements has made the broad utilization of pictures unavoidable. There are numerous approaches to give security to information that is being imparted. Stages that bolster such calculation on picture handling reasons for existing are called secure picture preparing conventions. In this postulation, we propose another security demonstrate that depicts a plan of successful security for correspondence by AES calculation for encryption and unscrambling. It depends on AES Key Expansion in which the encryption procedure is somewhat shrewd selective or operation of an arrangement of picture pixels alongside the 128 piece key which changes for each arrangement of pixels. In January, 1997 NIST started its push to build up the AES, a symmetric key encryption calculation, and made an overall open require the calculation to succeed DES.With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes.

Algorithm of AES:

- Step 1: To input an Image.
- Step 2: Convert this analog image into digital image.
- Step 3: Convert the image pixels into Row and Columns form.
- Step 4: Perform transpose of Columns.
- Step 5: Add these columns using bitwise-Xor operation.
- Step 6: Get the Output.

5. Conclusion and Future work

Security in transmission of digital images has its importance in today's image communications, due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue. In this paper detailed study of AES algorithm has been presented also provides compassion of different cryptographic algorithms. In future try to propose a novel mechanism in which AES algorithm will be apply to transmit images securely in image communication system.

References

[1] Kayhan CELİK and Erol KURT (2016): A New Image Encryption Algorithm Based on Lorenz System, ECAI 2016 - International Conference – 8th Edition Electronics, Computers and Artificial Intelligence, IEEE , pp: 23-28.

[2] Mohamed A. Mokhtar, Nayra M.Sadek and Amira G. Mohamed (2017), Design of Image Encryption Algorithm Based on Different Chaotic Mapping, 34th NATIONAL RADIO SCIENCE CONFERENCE, IEEE, pp: 197-204.

[3] Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, Yushu Zhang, Kwok-Wo Wong, Riccardo Rovatti and Gianluca Setti (2017): On the Security of a Class of diffusion Mechanisms for Image Encryption , IEEE, pp: 1-13.

[4] Yeter ŞEKERTEKİN, Özkan ATAN (2016): An Image Encryption Algorithm Using Ikeda and Henon Chaotic Maps, IEEE, pp: 1-4.

[5] Sushmita Singh and Musheer Ahmad, Dhruv Malik (2016): Breaking an Image Encryption Scheme Based on Chaotic Synchronization Phenomenon, IEEE, pp: 1-4.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki (2007): A Modified AES Based Algorithm for Image Encryption, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 1, No: 3, pp: 745-750.

[7] KirtiUpreti, Kriti Verma, and Anita Sahoo (2010): Variable Bits Secure System for Color Images, Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, IEEE, pp: 105-107.

[8] Xiang Fei and Guo Xiao-cong(2011): An Image Encryption Algorithm based on Scrambling and Substitution using Hybrid Chaotic Systems, Seventh International Conference on Computational Intelligence and Security, pp: 882-885.

[9] Rohit Joshi and Sumit Joshi (2011): Color Image Encryption through a Novel Chess Based Confusion Scheme using Chaotic Map, IEEE, pp: 444-448.

[10] P. Radhadevi and P. Kalpana (2015): Secure Image Encryption Using AES, International Journal of Research in Engineering and Technology, pp: 115-118.

[11] Roshni Padate and Aamna Patel (2015): Image Encryption and Decryption Using AES Algorithm, International Journal of Electronics and Communication Engineering & Technology, pp: 23-29.

[12] Wenying Wen, Yushu Zhang, Yuming Fang and Zhijun Fang(2016): A novel Selective Image Encryption Method Based on Saliency Detection, IEEE VCIP, pp: 1-4.

[13] YeterSekertekin and OzkanAtan (2016): An Image Encryption Algorithm Using Ikeda and Henon Chaotic Maps, 24th Telecommunications forum TELFOR, pp: 1-4.

[14] Anish Goel and KaustubhChaudhari (2016): Median Based Pixel Selection for Partial Image Encryption, IEEE, pp: 1-5.