SECURED IMAGE SYSTEM USING GRAYSCALE IMAGE ENCRYPTION

Miss. Switee N. Zambre
Department of Computer Engineering
Zeal College of Engineering and Research

Dr. Sunil M. Sangve
Department of Computer Engineering,
Zeal College of Engineering and Research.

Abstract—

In latest years, there is a speedy development in the multimedia and network technologies in computer era. Transmission of multimedia information over the network leads the major problems of security, privacy and data size. Images are widely used and the major problems are how to protect the images and also reduce size of the image in order to maximize the network utilization. Various techniques are there with a view to secure the image and to reduce the size of the image. Security and privateness aren't taken into consideration in the sooner Image compression techniques. To provide the privacy and security, the encryption is applied as well as compression reduces the data size. So that, to overcome the issues in multimedia and network technologies, compression is combined with encryption. In order to get higher network utilization, the encrypted images are compressed. An efficient image Encryption Then Compression (ETC) system is designed. In proposed scheme Advanced Encryption Standard algorithm is used to encrypt the image with the intention to get high security.

Index Terms—AES encryption algorithm, encryption, decryption, lossless Compression, decompression, security.

I. INTRODUCTION

A. BACKGROUND

Image processing is a technique to transform an image into digital form and perform some operations on it, as a way to get an enhanced image or to extract a few useful data from it. It is a type of signal dispensation wherein input is image, like video frame or photograph and output can be image or characteristics related to that image. Information Security is not all about securing data from unauthorized access. Information Security is basically the exercise of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of data. With the rapid improvement of multimedia and network technologies, the safety of multimedia becomes more important, since multimedia data are transmitted over open networks more frequently. Security of information to preserve its confidentiality, proper access control, integrity and availability is a major trouble in data communication.

Typically, reliable security is essential to content protection of digital images and videos. Encryption schemes for multimedia records need to be specially designed to protect multimedia content and fulfill the safety requirements for a selected multimedia application. For example, real-time encryption of an entire video stream using classical ciphers requires heavy computation because of the huge quantities of data involved, but many multimedia application require security on a much lower level, this will be achieved using selective encryption that leaves a few perceptual data after encryption. Image Encryption is the process of converting an image into unreadable format so that it could be transmitted over the network safely. Its reverse method is image decryption, which is used to convert the unreadable format of an image to the original image and for this the receiver have to use the key for the encrypted data. Image compression is defined as a process of reducing the image size.

B. MOTIVATION

To provide an image encryption mechanism which provides high security level, less computational time and in reliable and efficient way.

C. OBJECTIVES

1. To enhance the security against different types of Attacks.
2. To increase the image quality.
3. To increase the robustness and efficiency.

II. REVIEW OF LITERATURE

In this paper, an image encryption scheme primarily based on Multi-stage blocks scrambling is proposed. The photograph is first decomposed into non-overlapping, blocks and scrambling of these blocks is accomplished by the usage of 2D Cat Transform. [1].

In this Paper, proposed image encryption approach this consists of scrambling and diffusion stages. In scrambling stage, Input Image undergoes row scrambling and column scrambling with the help of chaotic map [2].

In this paper, compares lossless Encryption then Compression (ETC) technique which uses image encryption (i.e., RSA algorithm) used to encrypt the image by ensuring privacy in transmission without any malicious assaults and image compression. [3].

In this paper, it introduce a scheme for digital image scrambling based totally on the precept of information entropy. [4].

In this paper, proposed the Encryption-then-Compression Systems to safely transmit Images through an untrusted channel provider. It makes use of 8/8 blocks for block scrambling. [5].

In this research paper Fast Encryption Algorithm is modified to make it work on text and binary data. In the modification logic gate is modified to make key generation more secure. Also in this research FEAL is able to encrypt any type text of data where as previously it cannot work on text type of data, it was implemented only on gray scale images. Despite this, the FEAL can now be used for the encryption of colour images [6].

In this paper, the image encryption has been achieved through prediction error. A compression algorithm for encrypting image has been realized by the usage of 3 one of a kind wavelet transform techniques which include HAAR, BIOR and DAUBECHIES individually. After the test results suggests the HAAR wavelet offers the reasonably high safety level. The MSE, PSNR values and compression ratio for resultant images are better than the preceding one. Better results of peak signal to noise ratio indicates that the reconstructed image is of better quality [7].

This paper talks more about the algorithms related to the binary and gray code in terms of the digital image. Where the text file is attached and transformed into the grey code and cover it within the digital image and then decrypt it. This whole work is achieved by the use of Matlab Software, so there's no need of network conversation system. The differences between the authentic and the Stego images are prominent with the assist of PSNR and MSE values [8].

This paper implements secured and effectual medical image encryption algorithm based on RC4 and make use of the medical image storage and transmission [9].

The encryption of an image is accomplished via pixel prediction and secret key. Extreme compression of the encrypted image is carried out by the use of techniques, Arithmetic and Huffman coding [10].

III. PROPOSED METHODOLOGY

In Our System, we are providing the security to the image while transmitting over the internet.

A. Architecture

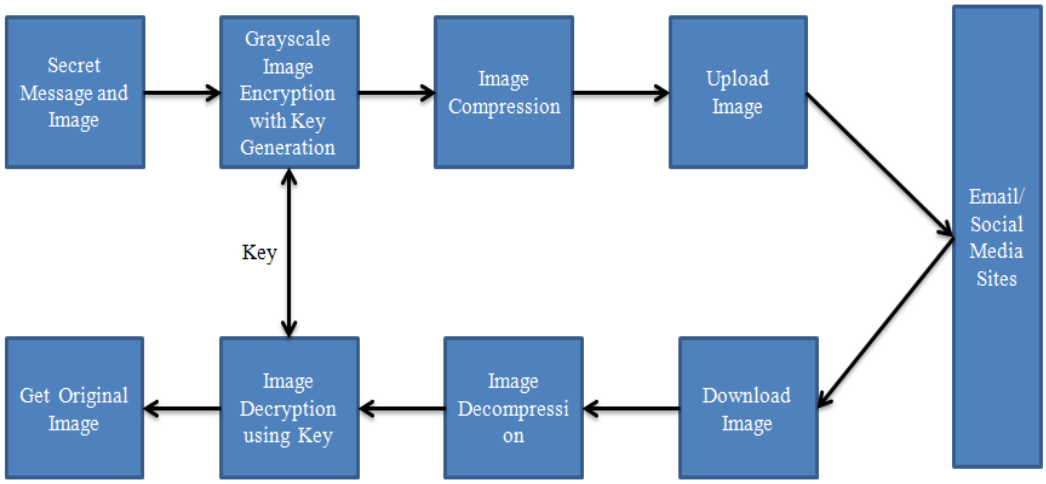


Fig: System Architecture

1) **Encryption:-** Image Encryption is the method of converting an image into unreadable format so that it may be transmitted over the network safely. Its reverse technique is image decryption, which is used to transform the unreadable format of an image to the original image and for this the receiver have to use the key for the encrypted data.

2) Compression:- Image compression is defined as a procedure of reducing the image size in accordance to a few loss of information. The two maximum extensively used image compression techniques are JPEG and JPEG 2000. We are JPEG 2000 for compressing the image.

3) Decompression:- Decompression technique restores the image to its original size.

4) Decryption:- Image Decryption process is image decryption, which is used to convert the unreadable format of an image to the original image and for this the receiver should use the important thing i.e., key for the encrypted data.

A. Module Explanation

Module 1 - Administrator (Admin):- Admin view user details. Give Authentication to users.
Module 2 - User:- User can upload the secret image.

B. Algorithms explanation

Advanced Encryption Standard:
1) Input:
2)128 bit /192 bit/256 bit input (0, 1)
3) Secret key (128 bit)+plain text(128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6) Xor state block (i/p)
7) Final round: 10, 12, 14
8) Each round consists : sub byte, shift byte, mix columns, add round key.
9) Output:
10)cipher text(128 bit)

C. Mathematical Model

1. Mathematical equation in Advanced Encryption Standard:
Initialization: password, key, time, salt : string
time ←− get time
input ←− (password)
key ←− salt + time
Encryption:
Ciphertext ←− AES Encrypt (password, key)
Output (ciphertext)
Decryption:
key ←− salt−time
for as much tolerance given time
if key = get time
key ←− salt + time
plaintext ←− AES Decrypt (ciphertext, key)
end if
end for
output (plaintext)

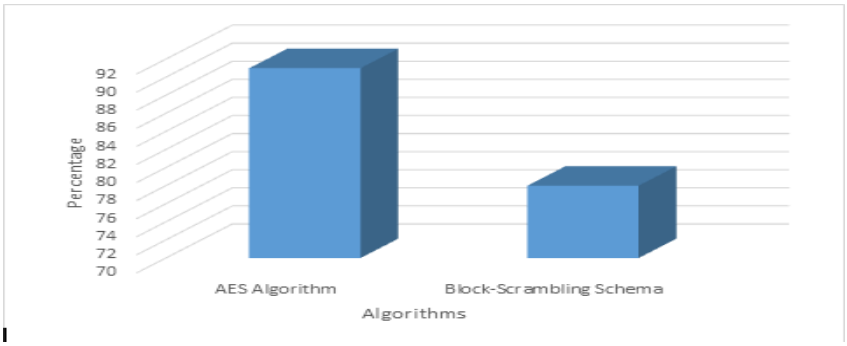
IV. RESULT AND DISCUSSION

I. Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i5-6700HQ CPU @ 2.60GHz, 16GB memory, Windows 7, MySql Server 5.1 and Jdk 1.8.

In our system, user will firstly upload the secret image to the system as an input. After that the secret image will get converted into unreadable format with the help of Advanced Encryption Standard Algorithm. Then the grayscale image will be reduced their size and upload it to the social media like facebook etc., then download it, after that we restores the original size of the input image and decrypt it to get the original image.

Result between Algorithms:

Sr. No	Algorithm	No. of images	Rate of grayscale	rate of data reduced	Result
01	Proposed System	30	29	29	89%
02	Existing System	30	23	21	76%



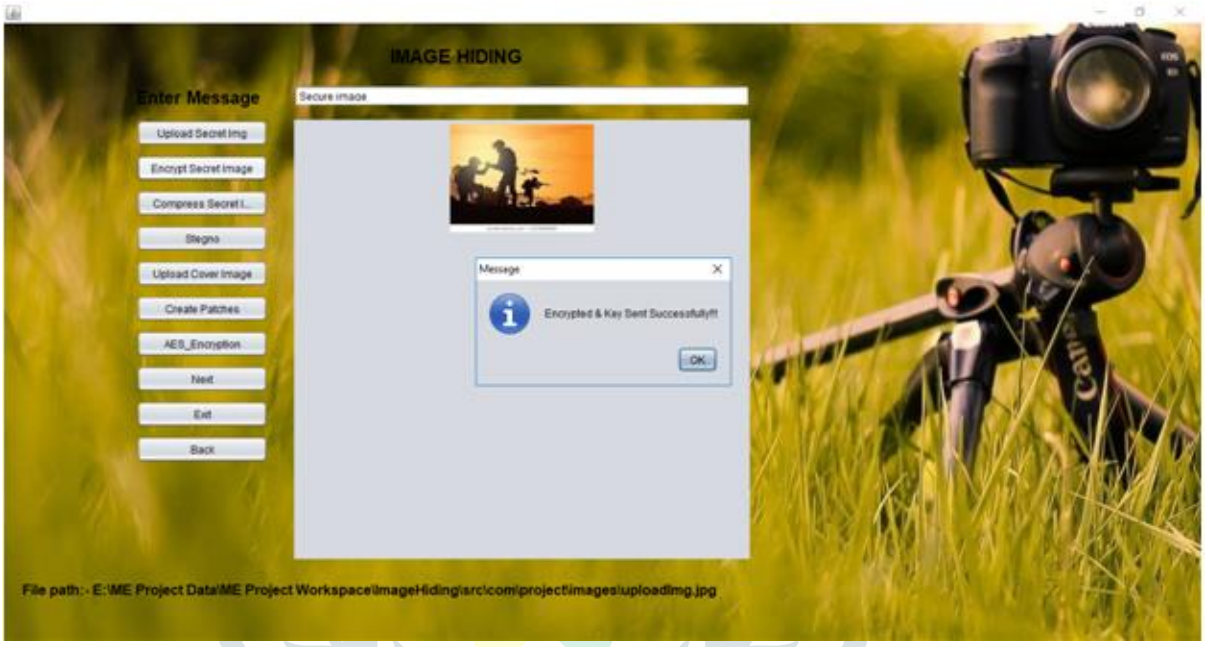


Fig: Secret image going to upload

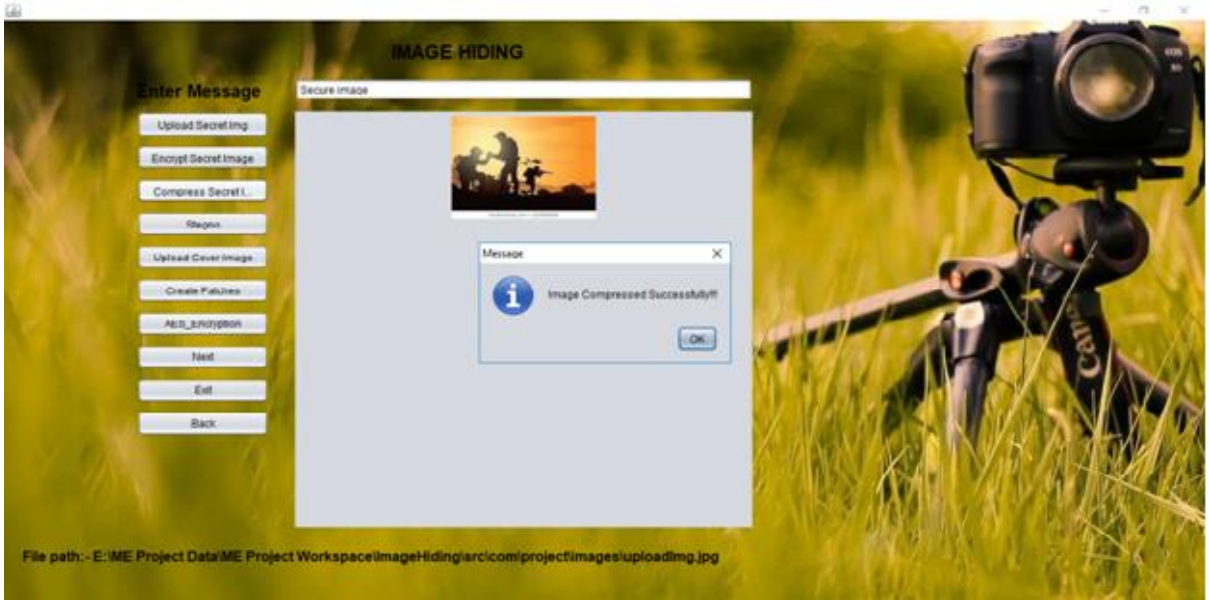


Fig: Compressed Secret Image

Fig: Decrypted image

V. CONCLUSION

We proposed a novel image encryption approach that enhances the security of systems for images and that image will be secured. The proposed scheme uses Advanced Encryption Standard algorithm to convert readable image into unreadable format i.e., grayscale. It enables the use of a smaller block size and a larger number of blocks than the color-based image encryption scheme. The Grayscale image reduces the size for taking less memory/space for travelling over the network.

REFERENCES

[1] Tatsuya Chuman, Warit Sirichotedumrong, ”Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images”, IEEE Transactions on Image Processing
(Volume: 28 , Feb. 2019).

[2] Musheer Ahmad, Omar farooq ”A Multi-Level Blocks Scrambling based Chaotic Image Cipher“, Department of Computer Engineering, ZH College of engineering and technology A.M.U. Aligarh-202 002.

[3] Usha salagundi, ”Image Encryption Using Scrambling and diffusion Operation Using Chaotic Map“ International Journal of Computer Science and Mobile Computing, Vol.5 May-2016.

[4] Priya C, Ramya C, Agashthiya R V, Hema R, Mythily G, Preethi V P ”An Efficient Method for Secure Image Compression“, International journal of Innovative Technology and Exploring Engineering(IJITEE) ISSN:22783075, Vol. 8, April 2019.

5] H. B. Kekre, Tanuja sarode, pallavi N. Halarnkar, ”Study of perfect Shuffle for Image Scrambling”, International Journal of Scientific and Research Publication Vol 4, February 2014.

[6] P. Nagabhushan, Prabhudev Jagadesh, R. Pradeep Kumar, ”A Novel Image Scrambling Technique Based On Information Entropy And Quad tree Decomposition“, International journal of Computer Science Issues(IJCSI) Vol 10 march 2013.

[7] Amarpreet Singh, ”Enhancement of Security in Data Mining Using FEAL (Fast Encryption Algorithm)”, International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7844-7846.

[8] Kritika Soni, Amit Kumar Manocha, ”An Efficient Image Encryption Then-Compression System via Wavelet Compression Technique” International Journal of Engineering Science and Computing, June 2016.

[9] Karthikeyan B, Asha S, Poojasree B, ”Gray Code Based Data Hiding in an Image using LSB Embedding Technique” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume8, Issue-1, May 2019.

[10] G. Saravana Kumar, V. Parthasarathy ,E. Praveen Kumar, S. Thiyagarajan, S. Siva Saravana Babu and S. Sudhakar, ”A Comprehensive Compression and Encryption Scheme for Secured Medical Images Communication” Indian Journal of Science and Technology, Vol 9(16).

[11] Bharath K P, Prabhavathi C ,” Efficient Grayscale Image Encryption Then Compression System” International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-4, Issue-6, Jun.-2016.