International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Encryption-then-Compression System with Watermarking

Miss. Aarti Harikishor Sharma Prof Dr. B. D. Phulpagar

Department of Computer Engineering P.E.S Modern College of Engineering Shivaji Nagar Pune-05

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Nowadays, nearly each man or woman inside the world are related to every other the use of Internet. Different files of photographs are transmitted through Internet for numerous applications. These photographs commonly include either personal or private data. Therefore, making sure confidentiality, integrity, authentication and non-repudiation of images at some stage in transmission is an important issue. In information processing field image security and image storage space requirements are two most of the widely explored field. To provide protection to the image many encryption algorithms were designed which might be different from the textual encryption algorithm. During data transmissions, these rather confidential records may be manipulated via an unauthorized person, as a result main to an insecurity for its sender. To overcome this problem, there are many techniques in which data hiding and image encryption are the two main strategies. We proposed a novel block-scrambling image encryption scheme that enhances the security of systems for JPEG images and that image will be secured.

Keywords: *Block scrambling encryption algorithm, Encryption, decryption, loss less Compression, decompression, security*

Introduction

Image processing is a method to transform an image into digital form and carry out 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 enter is image, like video frame or photo and output can be image or characteristics associated with that image. Information Security is not all about securing data from unauthorized access. Information Security is basically the exercise of stopping unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. With the rapid development of multimedia and network technologies, the safety of multimedia turns into more important, on account that multimedia information are transmitted over open networks more frequently. Security of data to hold its confidentiality, proper get admission to control, integrity and availability is a major trouble in data communication. Typically, dependable protection is critical to content protection of digital images and videos. Encryption schemes for multimedia records need to be particularly designed to protect multimedia content and fulfill the safety requirements for a specific 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

Protect data for your computer and also protect information in transit with Confidentiality of medical, private and transaction records in terms of image.

C. Objectives

1. To secure important information.
2. To increase the communication encryption.
3. To increase the efficiency.
4. Prevent data from getting stolen or read.

Review of Literature

In this research paper Fast Encryption Algorithm is modified to make it paintings on text and binary records. In the modification logic gate is changed to make key generation more secure. Also in this research

FEAL is capable of encrypt any kind textual content of information in which as previously it can't work on text type of facts, it become implemented only on grey scale images. Despite this, the FEAL can now be used for the encryption of coloration images [1].

In this paper, the picture encryption has been achieved via prediction error. A compression algorithm for encrypting photograph has been realized by the use of 3 certainly one of a type wavelet transform techniques which consist of HAAR, BIOR and DAUBECHIES individually. After the test outcomes suggests the HAAR wavelet offers the reasonably high safety level. The MSE, PSNR values and compression ratio for resultant pix are higher than the previous one.Better effects of peak signal to noise ratio suggests that the reconstructed photograph is of better quality [2].

This paper talks greater approximately the algorithms associated with the binary and gray code in terms of the digital photo. Where the text record is hooked up and transformed into the gray code and cover it in the digital photograph after which decrypt it. This whole work is achieved by the usage of Matlab Software, so there's no want of network communication system. The variations between the actual and the Stego pictures are prominent with the assist of PSNR and MSE values [3].

This paper has proposed the application of EtC systems, which enable customers to send pics securely to audience thru SNS companies. Moreover, we also look at how SNS providers manage JPEG images uploaded through customers in phrases of the maximum resolution of uploaded photographs and the parameters of recompression. The simulation effects showed that some block distortion due to recompression through SNS carriers heavily reduce photograph quality. On the alternative hand, it is confirmed that the EtC structures are applicable to almost all SNS vendors if encrypted photos meet some conditions [4].

This paper Novel block-scrambling picture encryption scheme that enhances the safety of EtC structures for JPEG photos. Although Bx = By = sixteen is used as the smallest block size in the conventional scheme to keep away from the impact of colour sub-sampling, the proposed scheme allows us to use Bx = By = 8 as a block size, which enhances robustness in opposition to ciphertext-simplest attacks. In comparison, decrypted pictures with the traditional scheme sometimes include some block distortion because of the interpolation on social media. The proposed scheme makes it viable to keep away from the impact of the interpolation on social media due to using grayscale-based snap shots [5].

This paper proposed an efficient ETC system for the JPEG XR standard. Four block-primarily based encryption steps have been used because the perceptual encryption schemes in the proposed system.We evaluated the safety of the proposed machine with its large key space. The experimental consequences confirmed that the proposed block size was appropriate for the JPEG XR compression and the proposed system accomplished both suited compression in cases of lossless and lossy compression and sufficient protection for stable image conversation while retaining the compatibility with the JPEG XR standard. Using the proposed system, the user can control the protection and the compression performance by deciding on a appropriate block length [6].

This paper Due to separation of information, needed for embedding and detection process, asymmetric watermarking is the best method today for public watermarking. Errors, introduced during watermark embedding and detection stages should be corrected using longer, supporting up to 3 error corrections in 4-bit message, error correction coding. Waveletbased watermarking scheme is robust against noise, lossless and DCT compression, filtering attacks due to the filtering properties of wavelet transformation. Testing of watermarked images shows that only coefficients of sub bands LH and HH retain watermark, while coefficients of sub band HL do not preserve the watermark and therefore cannot be taken into account, while testing images for presence of watermark [7].

In this Paper, proposed image encryption technique this includes scrambling and diffusion stages. In scrambling stage, Input Image undergoes row scrambling and column scrambling with the help of chaotic map [8].

In this paper, it introduce a scheme for digital image scrambling based on the principle of information entropy [9].

In this paper, an image encryption scheme based on Multi-level blocks scrambling is proposed. The image is first decomposed into non-overlapping, blocks and scrambling of these blocks is done by using 2D Cat Transform [10].

In this paper, author selects grey scale image to stimulate for encryption and compression. Author uses wavelet transform method of compression where its ability to describe any type of signals both in time and frequency domain and the image encryption has been achieved via prediction error clustering and random permutation [11].

In this paper, the encryption of an image is accomplished via pixel prediction and secret key. Extreme compression of the encrypted image is done by using two techniques, Arithmetic and Huffman coding. Due to use of extreame compression the image data are lost [12].

Proposed Methodology

We have worked to facilitate the information security in getting secure transmission of data/image over social media which maintain the information hiding inside texture image i.e., cover image. Hence this system is suitable for maintaining high level security for information transmission or image preservation in the network shown in Fig. 1.

In proposed work, a block scrambling technique is used to hide the image in RGB color to gray scale color image and also attach the cover image to the gray scale image for more security to the image. After the encryption of the image (gray scale image) compressed with lossless image compression to decrease the redundancy of the image thereby increasing the capacity of storage and efficient transmission. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed.

The proposed a block scrambling encryption scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

Architecture

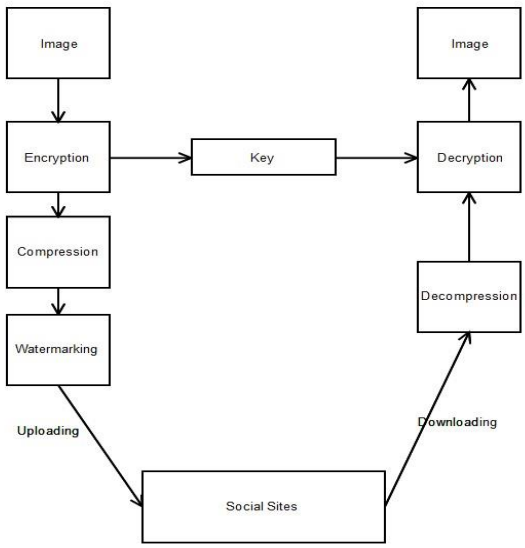


Fig. 1. Proposed System Architecture

The proposed system consists of three components:

1. Encryption: Image Encryption is the process of converting an image into unreadable format so that it can be transmitted over the network safely. Its reverse process 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.

2. Compression: Image compression is defined as a process of reducing the image size in accordance to some loss of information. The two most widely used image compression techniques are JPEG and JPEG 2000.

3. 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 have to use the key for the encrypted data.

A. Module Explanation

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

B. Algorithms explanation

1. Block-Permutation-Based Encryption (BPBE):

Step 1: Apply encryption to an original image I = {I_R, I_G, I_B} of M ×*Npixelsusingkeys.*

Step 2: Divide each color component of an original image into multiple blocks with B_x ×B_y By pixels.

Step 3: Permute the positions of the divided blocks randomly using keysK_2^R, K_2^G andK_2^B.

Step 4: Apply encryption using keys K_3^R , K_3^G andK_3^B.

Step 5: Rotate and invert each block randomly using keys
K_4^R , K_4^G,K_4^B, K_5^R, K_5^G, andK_5^B.

Step 6: Apply encryption using keys K_6^R, K_6^G andK_6^B.

Step 7: Apply the negative-positive transformation for each block using keysK_7^R, K_7^G andK_7^B.

Step 8: Apply encryption using keys K_8^R, K_8^G andK_8^B.

Step 9: Shuffle the three color components, i.e., R, G,and B in each block by using a key K_9.

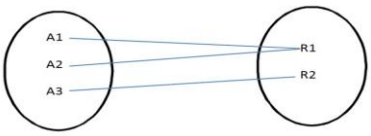
Step 10: Apply encryption using keys K_1^R0, K_1^G0 and K_1^B0.

Step 11: Generate the encrypted image IE = {I_{ER}, I_{EG}, I_{EB}} by integrating all the transformed blocks.

2. Compression:

$$Compression = \frac{Sizeofimagefile}{No.ofpixelsinoriginalimage} \quad (1)$$

C . Mathematical Model



Where,

A1: Query provided by the user. Eg: Secret Digital Image

A2: Query provided by user. Eg: Secret Digital Image

R1: Result provided by Encrypted-then-compressed Image.

A3: Wrong or incorrect data submitted

R2: Error occurred

Set Theory:

S= {s, e, X, Y,φ}

Where,

· *s = Startoftheprogram.*
· *Login.*
· *Uploadtheimage.*
· *Encryptionusingblock – scrambling.*
· *Compression.*
· *AttachCoverimagetodoublesecuretheimage.*
· *Recompression*
· *Decryption*
· *Logout*

e = End of the program. Resultant output provided by the
input image.

X = Input of the program. Input should be Image file i.e.,JPEG format.

Y = Output of the program.

Image will be uploading. Then the further processing will be done and finally appropriate result will provided.

X, Y U

Let U be the Set of System.
U= Client, I, E, C
Where, Client, I, E, C are the elements of the set. Client= User
I= Image
E= Encryption using Block-Permutation-Based Encryption (BPBE).
C= Compression.

Result and Discussion

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.

Table 1. Shows the comparison graph between existing system and proposed system algorithms. In our system, we provide security to the image/information over internet.

Accuracy between Algorithms

Table 1: Comparison

S.No	Algorithm	Accuracy
01	Proposed System	90%
02	Existing System	83%

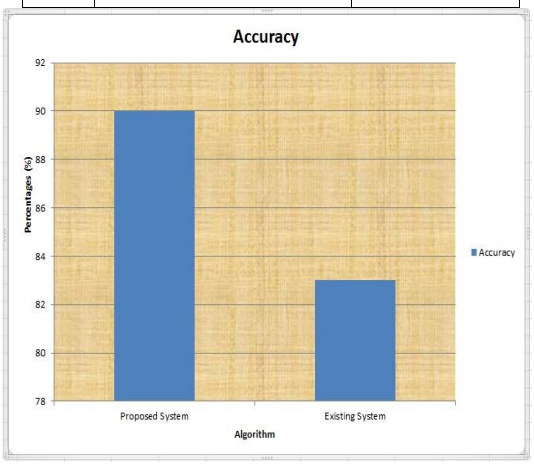


Fig. 2. Comparison graph

Conclusion

Preserving image safety has become an important trouble due to the fact transmission of information over the Internet arise very frequently. To provide security to the image the image is encrypted with encryption algorithm. We proposed a novel block-scrambling image encryption scheme that enhances the security of systems for JPEG images and that image will be secured. The proposed scheme enables the use of a smaller block size and a larger number of blocks than the color-based image encryption scheme. Images encrypted using the proposed scheme include less color information due to the use of gray scale images even when the original image has three color channels.

Acknowledgment

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University of Pune and concern members of CPGCON2020 conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1]. P. Nagabhushan, Prabhudev Jagadesh, R. Pradeep Kumar, "A Novel
[2]. Image Scrambling Technique Based On Information Entropy And Quad tree Decomposition", International journal of Computer Science Issues(IJCSI) Vol 10 march 2013.
[3]. 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.
[4]. Kritika Soni, Amit Kumar Manocha, "An Efficient Image EncryptionThen-Compression System via Wavelet Compression Technique" International Journal of Engineering Science and Computing, June 2016.
[5]. Tatsuya Chuman and Kenta Iida and Hitoshi Kiya, "Image Manipulation on Social Media for Encryption-then-Compression Systems" Proceedings of APSIPA Annual Summit and Conference 2017.
[6]. Warit Sirichotedumrong and Hitoshi Kiya, "Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images", journal of latex class files, vol. 14, no. 8, august 2015.
[7]. Kenta Kurihara, Osamu Watanabe, Hitoshi Kiya, "An Encryption-thenCompression System for JPEG XR Standard", 2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB).
[8]. Usha salagundi, "Image Encryption Using Scrambling and diffusion Operation Using Chaotic Map," International Journal of Computer Science and Mobile Computing, Vol.5 May 2016.
[9]. 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.
[10]. 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, Volume-8, Issue-1, May 2019.
[11]. 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.
[12]. Er. Maninder Kaur, Er. Navneet Choudhary, "A Research Paper On A Secure Image Encryption-Then Compression System Using Wavelet
[13]. Via Prediction Error Clustering And Random Permutation, Head of Department(CSE) Gurukul Vidyapeeth institute of Engineering and Technology, Banur Punjab Technical University, Jalandhar.
[14]. 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