Encryption-then-Compression with Watermarking

Aarti Harikishor Sharma, Prof Dr. B. D. Phulpagar
Department of Computer Engineering,
P.E.S Modern College of Engineering, Shivaji Nagar, Pune, India.

Abstract- Now a days, Nearly each man or woman inside the world are related to every other the use of Internet. Different files of photographs messages or data 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. We contrive the texture synthesis process into steganography to hide secret messages. 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 Block Permutation based Image Encryption scheme that enhances the security of systems for JPEG images and that image will be secured by using keys.

Index Terms- Block Permutation based Image Encryption Algorithm, Message, Encryption, Decryption, loss less Compression, Steganography, Decompression, Security, Keys and Watermarking.

I. 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 where in enter is image, like video frame or photo and output can be image or characteristics associated with that image. Security of data to hold its confidentiality, 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. 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.

Encryption then Compression systems allow us to securely transmit images through an un-trusted channel provider, such as social network service providers. Image Encryption is the most effective way to achieve data security. After encryption in order to read that file, We must have access to a secret (Key) that enables us to decrypt the file. Watermarking is the technique which used for protection of Digital Media, So that it can reduce the chances of attacks on original Data and enhance authenticity or integrity of the data. In this paper, we have proposed the Block Permutation Based Image encryption technique which will allow user to send the image with cover image along with patches.

This paper is organized as follows: Section II presents a review of background and related work. In Section III, Problem statement is given. In section IV, we introduce our proposed model. In Section V, we have shown the architecture diagram along with mathematical model. Section VI Presents System Analysis and Result. Finally, we summarize and conclude our work in Section VII.

II. LITERATURE REVIEW

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.
In this section, we briefly review the related work on Encryption then Compression using Grayscale image encryption for JPEG images.

In this paper Authors S.M. Mohidul Islam, Rameswar Debnath, S.K Alamgir Hossain proposed a Discrete Wavelet Transform (DWT) based digital image watermarking technique. For embedding process, we consider the watermark signal as a binary sequence which is embedded to the high (HL and HH)frequency band of the blue channel. For detecting process, the correlation between the high frequency band DWT coefficients of the watermarked image and the watermark signal is compared with the response as compared with the predefined threshold to determine whether the watermark is present or not. The experimental original image.results show that the method is comparatively robust to several attacks such as rotation, scaling, JPEG compression, cropping, and multiple watermarking.[1]

Gopi Krishnan S and Loganathan D proposed, new cryptographic scheme for securing color image based on visual cryptography scheme. A color image to be protected and a binary image used as key to encrypt and decrypt are taken as input. A secret color image which needs to be communicated is decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images are converted into binary image, and finally the obtained binary images are encrypted using binary key image, called as share-l to obtain binary cipher images. To encrypt Exclusive OR operation is done between binary key image and three half-tones of secret color image separately.[2]

This paper presents a new scheme for digital image scrambling based on the principle of information entropy by the Authors P. Nagabhushan, Prabhudev Jagadesh, R. Pradeep Kumar. The quad tree decomposition technique is used to hierarchically divide the image into blocks or regions for enforcing security at the block or region level of an image, Which thus ensures the security of the entire image. The experimental results show that the proposed algorithm can successfully scramble the images, and the analysis of the algorithm also demonstrate that the scrambled images have good information entropy and low correlation coefficients thereby satisfying the requisite security.[3]

In this paper authors Ambika Oad, Himanshu Yadav, Anurag Jain proposed survey on existing work which is used different techniques for image encryption and we also give general introduction about cryptography.[4]

In this paper Author Amarpreet Singh has proposed Fast Encryption Algorithm (FEAL) is an encryption/decryption technique used for the encryption/decryption of the grey scale images only. In this paper, FEAL is used for the encryption/decryption of colour images and text. In this, the key generation system for FEAL algorithm is updated using the XAND gate. By using the XAND gate, data cannot be deciphered using partial knowledge of key. This proposed system can also work upon the text data, which is firstly converted into bit sequence before making it an encrypted text. The comparison of the existing FEAL and proposed FEAL shows that the time taken by the proposed FEAL for the encryption /decryption of the grey scale image is less than that of the existing FEAL[5]

H. B. Kekre, Tanuja sarode, pallavi N. Halarnkar proposed many approaches for image encryption that have high security as well as simple encryption process have been proposed. In this paper, Perfect shuffle for image scrambling is introduced. Effects of perfect shuffles with different factors of the image size are discussed. The number of iterations required to get back the original image are related to the power of 2 Finally all these results are displayed by using 1024 X1024 Lena's image.[6]

In this paper authors R. Gayathri, Dr. V. Nagarajan proposed watermarking is used for providing the double security of image shares. The share is embedded into the host image using Least Significant Bit Insertion Technique (LSB). The scheme provides more secure and meaningful secret shares that are robust against a number of attacks. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR), histogram analysis and also numerical experimentation suggests that embedding time varies linearly with message length. The simulation results show that, the proposed system provides high level of security.[7]

In this paper Authors S.Shunmugan, P.Arockia Jansi Rani proposed the concept of image compression after encryption and study about the various technologies applied on encryption-then compression technology. It is also analyses the various secured compression technologies and can be applied to different types of images. This survey addresses the recipe for the secured image compression technologies based on JPEG, JPEG2000 and JPEG XR and presents the pros and cons of those secured image compression technologies. To choose the best technology for the secured image compression some general strategies are suggested based on this survey.[8]

Kritika Soni, Amit Kumar Manocha has proposed an efficient image encryption-compression system is designed. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. A new image compression algorithm is also implemented using Haar Wavelet Transform which efficiently compresses the encrypted image. By Using Haar wavelet transform with ETC there is better compression efficiency. The approach applied in this paper is proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR). For implementing the proposed algorithm, the Image Processing Toolbox under MATLAB software is used.[9]

Authors Kenta Kurihara, Osamu Watanabe, Hitoshi Kiya proposed The proposed encryption method can provide approximately the same compression performance as that of JPEG XR compression without any encryption. It is also shown that the proposed system consists of four block-based encryption steps, and provides a reasonably high level of security. Most of conventional perceptual encryption methods have not been designed for international compression standards, but for the first time this paper focuses on applying the JPEG XR standard, which supports lossy and lossless coding for various kinds of images including high dynamic range images.[10]

In this paper author Usha Salmagundi has proposed image encryption technique which includes scrambling and diffusion stages. In scrambling stage, Input image undergo row scrambling and column scrambling with the help of chaotic map.In diffusion stage manipulating the pixels value based on parity function. The result shows that proposed method achieves good security in terms of entropy and NPCR. Decryption is the reverse process of encryption.[11]

Authors Tatsuya Chuman and Kenta Iida and Hitoshi Kiya proposed the EtC systems are applied to social media like Twitter, that are known for carrying out some image manipulation. Block scrambling-based encryption schemes used in the EtC systems are evaluated in terms of the robustness against image manipulation on social media. This work aims to investigate how each social networking service (SNS) provider manipulates images, and to consider whether the encrypted images uploaded to SNS providers can avoid to include some distortion under the image manipulation. In the experiment, encrypted and non-encrypted JPEG images are uploaded to various SNS providers to confirm the robustness of EtC systems. It is shown that the EtC systems are applicable to almost all SNS providers.[12]

In this paper Authors Warit Sirichotedumrong, Tatsuya Chuman and Hitoshi Kiya proposed Images encrypted using the proposed scheme include less color information due to the use of grayscale images even when the original image has three color channels. These features enhance security against various attacks, such as jigsaw puzzle solver and bruteforce attacks. Moreover, it allows the use of color sub-sampling, which can improve the compression performance, although the encrypted images have no color information. In an experiment,
encrypted images were uploaded to and then downloaded from Facebook and Twitter, and the results demonstrated that the proposed scheme is effective for EtC systems, while maintaining a high compression performance.[13]

Authors Karthikeyan B, Asha S, Poojasree B proposed the digital image steganography because of its demand and availability,where images are in the form of pixels and can be represented in the form of binary. Since technology is developed, hackers also got developed. Therefore the security must be implemented in a better manner. To overcome the hackers, Gray code based technique is used to conceal a text in the digital image and then decrypt it. The proposed algorithm is implemented in MATLAB. This paper point is to transfer a confidential data in best and secure way where no one can recover the private information and also we can differentiate the images by using PSNR and MSE.[14]

In this paper WaritSirichotedumrong,Tatsuya Chuman,Hitoshi Kiya proposed the scheme enables the use of a smaller block size and a larger number of blocks than the conventional scheme. Images encrypted using the proposed scheme include less color information due to the use of grayscale images even when the original image has three color channels. These features enhance security against various attacks such as jigsaw puzzle solver and brute-force attacks. In an experiment, the security against jigsaw puzzle solver attacks is evaluated. Encrypted images were uploaded to and then downloaded from Facebook and Twitter, and the results demonstrated that the proposed scheme is effective for EtC systems.[15]

III. PROBLEM STATEMENT

There are some encryption techniques where the images are divided into 8x8 blocks and at the output end the image will be not secure and also the image get blurred. Data also get lost in the existing work.

In Existing System there is limitation on block size to prevent JPEG distortion due to recompression forced by social media. In Proposed scheme, we have tried to solve this limitation.

IV. PROPOSED METHOD

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.

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.

The proposed system consists of following 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. **Steganography:**Steganography process is used to hide the secret message in image and also extract the secret message from texture image in our system

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 have to use the key for the encrypted data.

V. SYSTEM ARCHITECTURE

In System architecture secret message is going to be hide in the secrt image and after that all the operations can be carried out on the image. Image will be the original image that sender wants to encrypt. Then on the image encryption, compression operations will be performed. After all the operations ,cover image will be uploaded on the original image and patches will be created on the image and will be sent to the receiver with the encrypted secret key. over real time sharing on mail. And after that all the reverse operations will be performed on that image by receiver side while doing decryption.

This many high security will be provided to the original image so that the decryption time will increase for the decrypting the image while doing attacks.

The architectural diagram is as follows.

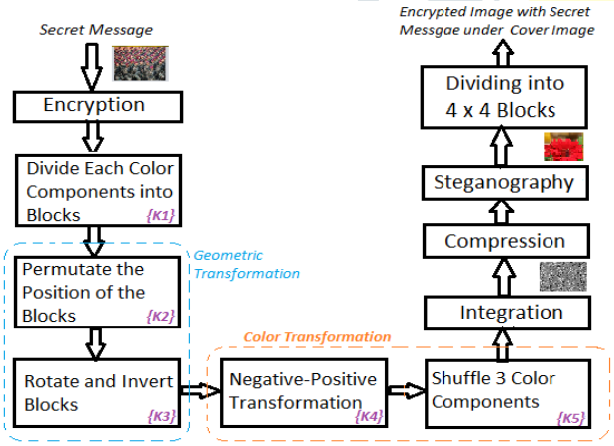


Fig 1: Proposed System Architecture

A. Advantages of Proposed System

- The recovered source texture image is exactly the same as the original source texture, so no loss of pixels in this process.
- Reducing distortion is the crucial issue in existing method this will overcome by our system.
- System provides the security to the important file and documents on which there is a chance of hack or attack by the attackers.
- To share digital image as well as message(data) without risk and noiseless at time of transmission without effecting the original feature of the digital images

B. Project Modules

User Module:

- User first register account in application.
- After activating account, user should login.
- User will enter the secret message and will upload the secret image.
- Encryption and compression will be perform on image.
- After processing user gets the extracted original image and message result.

Admin:

- Uploaded image encryption.
- Image Compression.
- Uncover Watermarked Image.
- Secret Image Extraction
- Secret Message Extraction.

C. Algorithm

1. Block-Permutation-Based Encryption (BPBE): Step 1: Apply encryption to an original image I = {IR, IG, IB} of M ×Npixelsusingkeys.

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

Step 3: Permute the positions of the divided blocks randomly using keys KR 2 , KG 2 and KB 2 .

Step 4: Apply encryption using keys KR 3 , KG 3 and KB 3 .

Step 5: Rotate and invert each block randomly using keys KR 4 , KG 4 ,KB 4 , KR 5 , KG 5 , and KB 5 .

Step 6: Apply encryption using keys KR 6 , KG 6 and KB 6 .

Step 7: Apply the negative-positive transformation for each block using keys KR 7 , KG 7 and KB 7 .

Step 8: Apply encryption using keys KR 8 , KG 8 and KB 8 .

Step 9: Shuffle the three color components, i.e., R, G,and B in each block by using a key K9.

Step 10: Apply encryption using keys KR 1 0, KG 1 0 and KB 1 0.

Step 11: Generate the encrypted image IE = {IER, IEG, IEB} by integrating all the transformed blocks.

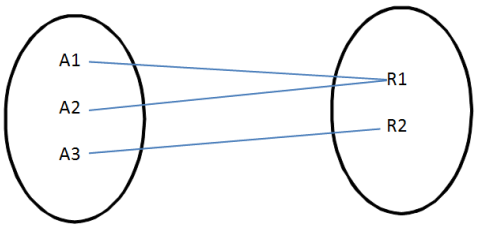
2. Compression:

Compression Ratio (CR) is the ratio between reconstructed file size and input file size. For any algorithm compression Ratio (CR) should be higher in order to achieve better compression.

Compression Ratio =

$$\frac{\text{Size of image file}}{\text{No. of pixels in original image}}$$

D. 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,phi}

Where,

- s = Start of the program.
- Log in.
- Upload the image.
- Encryption using block-scrambling.
- Compression.
- Attach Cover image to double secure the image.
- 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 be provided.

X, Y ∈ U

Let U be the Set of System.

U= {Client, M, I, E, C, St}

Where, Client,M, I, E, C,St are the elements of the set.

Client= User

M=Message

I= Image

E= Encryption using Block-Permutation-Based Encryption (BPBE).

C= Compression.

St=Steganography

VI. SYSTEM ANALYSIS AND RESULT

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3- 2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and jdk 1.8. This application is desktop application used tool for design code in Eclipse and execute.

Fig 2: Original Image

Fig 3: Encrypted Image with cover Image

Fig 4:Patches

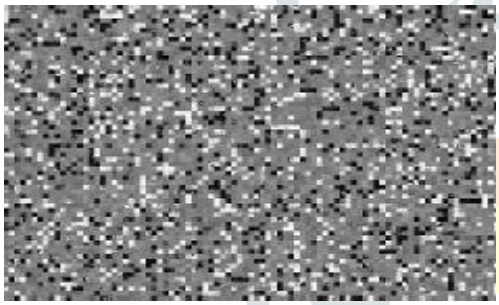


Fig 5: Encrypted Image

Table1: Properties of Block Scrambling Encryption and Block Permutation based Encryption.

Scheme	Existing	Proposed
Color Channel	RGB	Grayscale
Algorithm	Block Scrambling	Block Permutation based Encryption
Cover Image	No	Yes
Data Hiding	No	Yes
Effect of Color sub-sampling	Affected	Not Affected
Robustness against Attacks	Robust	More Robust

Table2: Result of Input Image Processed by using different Image Size and Color.

Image	Original Image	Cover Image	Result
Image Size(Pixels)	1000x1000	1000x1000	Image will encrypt successfully
	>1000x1000	1000x1000	Bound must be positive
	<1000x1000	>1000x1000	Bound must be positive
Image Color	RGB	Block and white	Image will encrypt successfully
	RGB	RGB	Image will encrypt successfully
	Black and white	Black and white	Image will encrypt successfully

VII. CONCLUSION

The message and image is loaded by using GUI format. Secret Image as well as secret message will be extracted by the receiver on the decryption by using Key. Proposed methodology uses Steganography for hiding data inside the image which input the texture image pattern for hiding text in the image and covering the original image with watermarking technique. Reducing distortion is the crucial issue in existing method this will overcome by our system by using smaller blocks and improves the image quality on decryption. To provide security to the image, The image is encrypted with Block Permutation based Image Encryption Algorithm that enhances the security of systems for JPEG images. 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. We have compared our results with the results obtained by previous work, which is giving best results and higher percentage of image security.

REFERENCES:

[1] S.M. Mohidul Islam, Rameswar Debnath, S.K Alamgir Hossain,"DWT Based Digital Watermarking Technique and its Robustness on Image Rotation, Scaling, JPEG compression, Cropping and Multiple Watermarking",International Conference on Information and Communication Technology
ICICT 2007, 7-9 March 2007.

[2] Gopi Krishnan S and Loganathan D,"Color Image Cryptography Scheme Based on Visual Cryptography",Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)

[3] 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.

[4]Ambika Oad, Himanshu Yadav, Anurag Jain,"A Review: Image Encryption Techniques and its Terminologies",International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[5] 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.

[6]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.

[7]R. Gayathri, Dr. V. Nagarajan,"Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme",IEEE ICCSP 2015 conference.

[8]S.Shunmugan, P.Arockia Jansi Rani,"Encryption-then-Compression Techniques: A Survey",International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)2016.

[9] Kritika Soni, Amit Kumar Manocha, "An Efficient Image EncryptionThen-Compression System via Wavelet Compression Technique" International Journal of Engineering Science and Computing, June 2016.

[10] Kenta Kurihara, Osamu Watanabe, Hitoshi Kiya, "An Encryption-then-Compression System for JPEG XR Standard", IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)2016.

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

[12]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.

[13] Warit Sirichotedumrong, Tatsuya Chuman and Hitoshi Kiya,"Grayscale-Based Image Encryption Considering Color Sub-sampling Operation for Encryption-then-Compression Systems",2018 IEEE 7th Global Conference on Consumer Electronics (GCCE 2018).

[14] 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.

[15]Tatsuya Chuman, Warit Sirichotedumrong, Hitoshi Kiya, "Encryption then Compression systems using grayscale based image encryption for JPEG Images",IEEE Transactions on Image Processing (Volume: 28 , Feb. 2019).