

Modified scheme for Lossy Compression and Iterative Reconstruction for Encrypted Image

¹Asha P. Ghodake, ²Sujata Mendgudle

¹Bharati Vidyapeeth College of Engineering, Navi Mumbai, India

²Ramrao Adik Institute of Technology, Navi Mumbai, India

Abstract

This paper presents advanced scheme for lossy compression of an encrypted image with flexible compression ratio. Encryption of original image is obtained by using pseudorandom permutation. Then encrypted image is compressed by using orthogonal transform and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount. After receiving the compressed image, receiver can reconstruct the principle contents of original image by iteratively updating the values of coefficients. For this process flexible compression ratio is used. The compression ratio and the qualities of the reconstructed image are dependent on the values of compression parameters. Higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. The proposed scheme significantly improves the compression efficiency.

Keywords

Lossy Compression, Orthogonal Transform, Compression Ratio, Encryption

I. Introduction

Now a day's, large files such as digital images to be easily transmitted over the internet. The security of digital images involves several different aspects. Encryption is used for content confidentiality and access control through which only authorized parties holding decryption keys can access content in clear text. The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form [1].

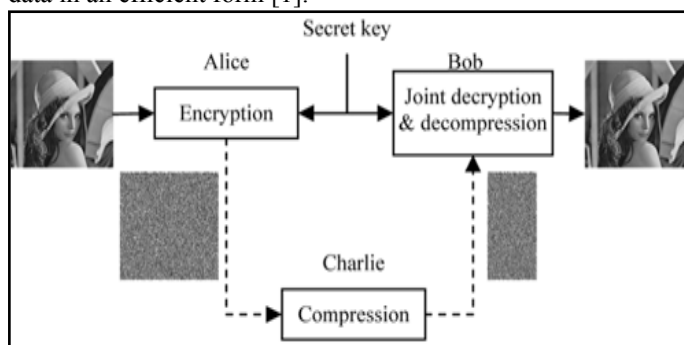


Fig. 1: Secure Transmission of Redundant Data

A pseudorandom permutation is used to encrypt an original image. In this, pixel position is changed and the encrypted data are efficiently compressed by orthogonal transform and discarding the excessively rough and fine information. After receiving the compressed data, reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image [2].

There are different methods of encryption and compression. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data [3]. In existing system for

image encryption, unencrypted plain-text image X_n is described by n bits a key sequence K_n of the same dimension as the plain-text, consisting of bits selected uniformly at random. The image is encrypted by applying a bitwise exclusive-OR (XOR) between each key bit and the corresponding plain-text bit to produce the cipher-text $Y_n = X_n \oplus K_n$. In this system, standard stream-cipher encryption and LDPC codes are used for compression [4].

II. System Overview

Encrypt an original image using pseudorandom permutation, and then encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. A receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients.

A. Image Encryption

Image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. In this method, the pixel values are same after encryption but their position will be changed. Image and video encryption have applications in various fields [5]. The original image is in uncompressed format and each pixel with a gray value falling into $[0, 255]$ is represented by 8 bits. Denote the numbers of the rows and the columns in the original image as N_1 and N_2 , and the number of all pixels as $N = N_1 \times N_2$. Then, the amount of bits of the original image is $N \times 8$.

Number of pixels = $N = N_1 \times N_2$

Number of bit = $N \times 8$

B. Compression of Encrypted Image

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression may be lossy or lossless.

Lossy methods are especially suitable for natural images such as photographs, compress multimedia data (audio, video, and still images). In the proposed scheme, a majority of pixels are converted to a series of coefficients using an orthogonal transform, and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount. In orthogonal transform convert image pixel values to transform coefficient values. This is a linear process and no information is lost, the number of coefficients produced is equal to the number of pixels transformed.

C. Steps for Compression of Encrypted Image

1. The network provider divides Permuted pixel sequence, into two parts: the first part made up of $(\alpha \cdot N)$ pixels and the second one containing the rest of the $(1 - \alpha) \cdot N$ pixels. The pixels in the first part are called rigid pixels and the pixels in the second part

are elastic pixels. It is called decomposition.

2. Pixels in first part as $p_1, p_2, p_3, \dots, p(\alpha \cdot N)$ and pixels in second part as $q_1, q_2, \dots, q_{(1-\alpha) \cdot N}$.

The value of α is within $(0, 1)$.

3. Perform an orthogonal transform in the elastic pixels to calculate the coefficients

$$Q_1, Q_2, \dots, Q_{(1-\alpha) \cdot N} \\ [Q_1, Q_2, \dots, Q_{(1-\alpha) \cdot N}] = [q_1, q_2, \dots, q_{(1-\alpha) \cdot N}] \cdot H$$

Here, H is a public orthogonal matrix with a size of $(1 - \alpha) \cdot N \times (1 - \alpha) \cdot N$ and it can be generated from orthogonalizing a random matrix.

Size of $H = (1 - \alpha) \cdot N \times (1 - \alpha) \cdot N$

4. For each coefficient Q , calculate

$$S_k = \text{mod} \left[\text{round} \left(\frac{Q_k}{\Delta} \right), M \right]$$

$k = 1, 2, \dots, (1 - \alpha) \cdot N$

Where Δ and M are system parameters.

The round operation returns the nearest integer and the mod operation gets the remainder. Q_k is converted into an integer S_k within

$[0, M - 1]$.

5. Then $Q_k = r_k \cdot \Delta + S_k \cdot (\Delta/M) + t_k$

r_k = rough information and

t_k = fine information

The rough information r_k and the fine information t_k are discarded.

While only the information S_k on the medium level remains.

The rough information r_k will be retrieved by an iterative image reconstruction procedure, and the loss of the fine information t_k cannot seriously affect the quality of the reconstructed image,

Where

$$0 \leq S_k \leq M - 1 \\ -\left(\frac{\Delta}{2M}\right) \leq t_k < \left(\frac{\Delta}{2M}\right)$$

6. Segment the set of s_k into many pieces with $L1$ digits and calculate the decimal value of each digit piece. Then, convert each decimal value into $L2$ bits in a binary notational system, where

$$L2 = [L1 \cdot \log_2 M]$$

The total length of bits generated from all pieces of s_k is

$$L = (1 - \alpha) \cdot N \cdot \log_2 M$$

Then each value of s_k is represented by $\log_2 M$ bits.

7. Collect the data of rigid pixels, the bits generated from all pieces of S_k , and the values of parameters including $N1, N2, \alpha, \Delta, M$ and $L1$ to produce the compressed data of encrypted image. Compression ratio R is a ratio between the amounts of the compressed data and the original image data, is approximately

$$R = \frac{8 \cdot \alpha \cdot N + \log_2 M \cdot (1 - \alpha) \cdot N}{8 \cdot N} \\ = \alpha + \frac{\log_2 M}{8} (1 - \alpha)$$

D. Image Reconstruction

In this system, iterative reconstruction is used because iterative approach includes improved insensitivity to noise and capability of reconstructing an optimal image in the case of incomplete data with the compressed data and the secret key.

E. Steps of Image Reconstruction

1. Decompose the compressed data and obtain the gray values of rigid pixels, the values of all S_k , and the values of parameters.

Here, with the knowledge of M and $L1$, the receiver may calculate $L2$, and then get the values of S_k by converting binary blocks with $L2$ bits into digit pieces in an M -ary notational system. Obtain S_k and all the parameters from compressed data.

2. According to the secret key, the receiver can retrieve the positions of rigid pixels. That means the original gray values at the positions, which distribute over the entire image, can be exactly recovered.

3. For the pixels at other positions, i.e., the elastic pixels, their values are firstly estimated as the values of rigid pixels nearest to them. That means, for each elastic pixel, we find the nearest rigid pixel and regard the value of the rigid pixel as the estimated value of the elastic pixel. If there are several nearest rigid pixels with the same distance, regard their average value as the estimated value of the elastic pixel. Because of spatial correlation in the natural image, the estimated values are similar to the corresponding original values. In the following, the estimation will be iteratively updated by exploiting the information of S_k .

4. Rearrange the estimated values of elastic pixels using the same permutation way, and denote them as $q'_1, q'_2, \dots, q'_{(1-\alpha) \cdot N}$.

5. Calculate the coefficients

$$[Q'_1, Q'_2, \dots, Q'_{(1-\alpha) \cdot N}] \\ = [q'_1, q'_2, \dots, q'_{(1-\alpha) \cdot N}] \cdot H$$

6. Calculate the differences

$$dk = \text{mod} \left[\left(\frac{Q'_k}{\Delta} \right), M \right] - S_k$$

$k = 1, 2, \dots, (1 - \alpha) \cdot N$

7. Modify the coefficients to the closest values consistent with the corresponding S_k .

8. Perform inverse transform

$$[q''_1, q''_2, \dots, q''_{(1-\alpha) \cdot N}] \\ = [Q''_1, Q''_2, \dots, Q''_{(1-\alpha) \cdot N}] \cdot H^{-1}$$

9. Calculate the average energy of difference between the two versions of elastic pixels

$$D = \frac{1}{(1 - \alpha) \cdot N} \cdot \sum_{k=1}^{(1-\alpha) \cdot N} (q''_k - q'_k)^2$$

- If D is greater than a threshold T (recommended 0.05), go back to step 5 –iterating.
- Otherwise, terminate the iteration and output the image made up of the rigid pixels and the final version of elastic pixels.

III. System Design

1. In encryption the pixel values are same after encryption but their position will be changed.

2. Permuted pixels are divided into rigid and elastic pixels. Perform orthogonal transform in elastic pixels. Remove rough and fine information and keep S_k . Finally collecting all data calculate compression ratio.

3. In reconstruction according to the secret key, the receiver can retrieve the positions of rigid pixels.

4. For each elastic pixel, we find the nearest rigid pixel and regard the value of the rigid pixel as the estimated value of the elastic pixel. If there are several nearest rigid pixels with the same distance, regard their average value as the estimated value of the elastic pixel. Because of spatial correlation in the natural image, the estimated values are similar to the corresponding original values.

5. Modify the coefficients to the closest values consistent with the corresponding S_k .

7. Perform inverse transform.

8. Calculate the average energy of difference between the two versions of elastic pixels.

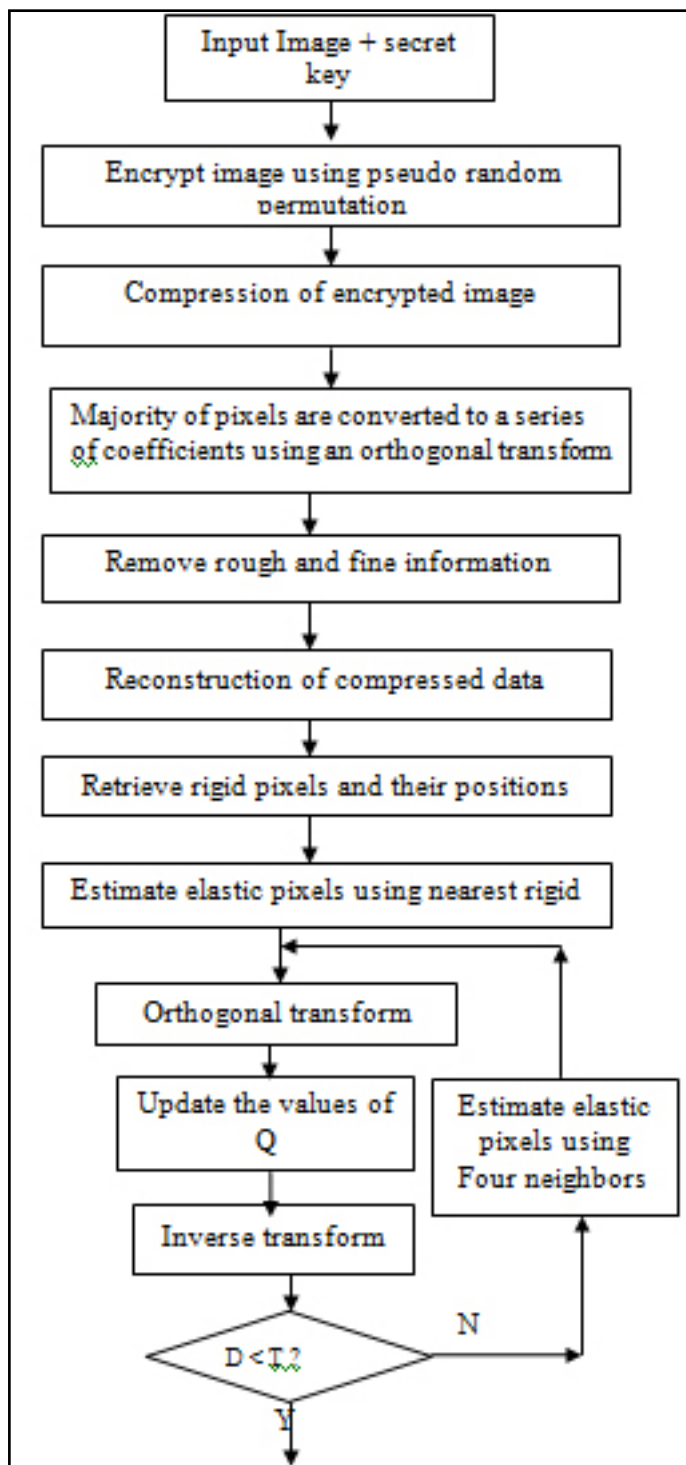


Fig. 2: Total Procedure of Encryption, Compression and Reconstruction

IV. Result

The test image Lena, shown in fig. 3(a) sized 512 x 512 used as the original image. After pixel permutation, the encrypted data of the image were produced, fig. 3(b). For showing their disorder, the encrypted pixel sequence is rearranged as a matrix with size of 512 x 512. Then, we compressed the encrypted data with different values of α and M and then calculate the compression ratio R with different values of α and M . With the compressed data, the receiver can retrieve the original content by using the image reconstruction procedure, fig. 3(c) and fig. 3(d). In which all rigid pixels are recovered and the elastic pixels are estimated as the values of their nearest rigid pixels.

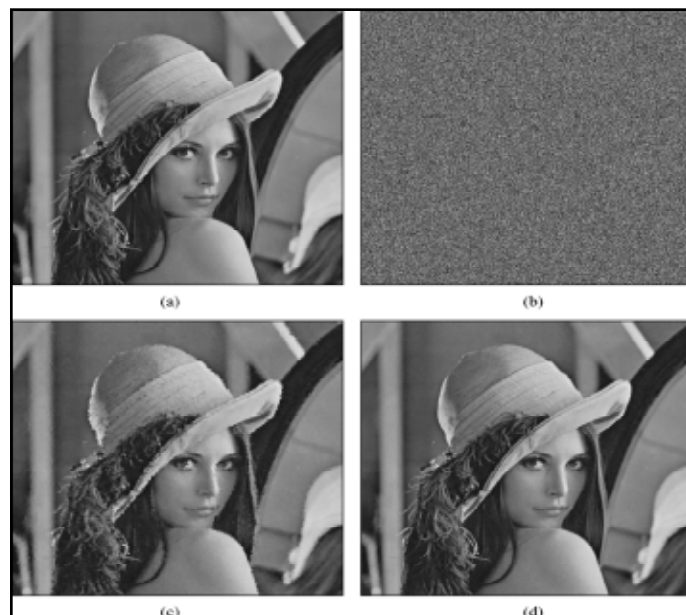


Fig. 3: (a) Original image Lena, (b) its encrypted version, (c). the medium reconstructed image from compressed data with less PSNR, and (d) the final reconstructed image with more PSNR

By collecting all data, we have calculated compression ratio R for original image Lena, as shown in Table 1.

Table 1: Compression ratio R in Reconstructed Image with Different Parameters for Test Image Lena

	α	R
$M = 7$	0.16	0.45
$M = 7$	0.12	0.42
$M = 7$	0.09	0.40
$M = 6$	0.16	0.43
$M = 6$	0.12	0.40
$M = 6$	0.09	0.38
$M = 4$	0.16	0.37
$M = 4$	0.12	0.34
$M = 4$	0.09	0.31

V. Conclusion

In this work, image encryption is obtained by changing the position of pixels. Performing orthogonal transform in permuted pixels and then removing rough and fine information compression is obtained. In iterative procedure in each step update the values of coefficients and reconstruction of original principal content. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

References

- [1] A. Mitra, Y. V. Subba Rao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering, 1, 2 pp. 127-131, 2006.
- [2] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE transactions on Information Forensics and Security, Vol. 6, No. 1, March 2011.

- [3] Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", IEEE Transactions on Image Processing, Vol. 19, No. 4, pp. 10971102, April 2010.
- [4] D. Schonberg, S. C. Draper, C. Yeo, K. Ramchandran, "Toward compression of encrypted images and video sequences", IEEE Transactions Information Forensics Security, Vol. 3, No. 4, pp. 749–762, Dec. 2008.
- [5] Daniel Schonberg, Stark C. Draper, Chuohao Yeo, Kannan Ramchandran, "Towards Compression of Encrypted Images and Video Sequences".
- [6] Ibrahim Fathy El-Ashry, "Digital Image Encryption", A Thesis Submitted for The Degree of M. Sc. of Communications Engineering.

Asha Pandit Ghodake received her B.E. degree in Electronics from Shivaji University, Kolhapur, Maharashtra in 2005. Currently she is persuing M.E. from University of Mumbai, Mumbai under the guidance of Prof. Sujata Mendgudle. She is currently working as Asst. Professor, with Department of Electronics & Telecommunication Engineering, Bharati Vidyapeeth College of Engineering, University of Mumbai, Mumbai from 2010. Earlier she worked with SSPM's College of Engineering, University of Mumbai, Mumbai from 2007 to 2010. Her research interests include digital signal processing and microwave.

Sujata Mendgudle received her B.E. degree in Electronics from Shivaji University, Kolhapur, Maharashtra in 1998 and M.E. from BATU, Lonere in year 2005. She is currently working as Asst. Professor, with Department of Electronics Engineering, Ramrao Adik Institute of Technology, University of Mumbai, Mumbai. Her research interests include digital signal processing and microwave.