Security and Privacy of Image by Encryption, Lossy Compression and Iterative Reconstruction

Asha P. Ghodake
Bharati Vidyapeeth College of Engineering
Navi Mumbai - 400614

Sujata Mendgudle
Ramrao Adik Institute of Technology
Navi Mumbai - 400706

ABSTRACT
Now a days, large files such as digital images, to be easily transmitted over the internet. New problems associated with this are security and privacy of image. Using pseudorandom permutation, image encryption is obtained. Confidentiality and access control is done by encryption. Encrypted image is compressed by using orthogonal transform. Irrelevance and redundancy of the image data is reduced by image compression because this is easy to store or transmit data in an efficient form. Reconstruct the original image by iterative reconstruction procedure. In this, flexible compression ratio is used and significantly improves the compression efficiency.

Keywords
Pseudorandom permutations, encryption, orthogonal transform, iterative reconstruction

1. INTRODUCTION
The presence of computer networks has prompted new problems with security and privacy. The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. The security of digital images involves several different aspects, including copyright protection, authentication, confidentiality and access control. Content confidentiality and access control are addressed by encryption, 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].

This work proposes a scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can 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. This ratio gives an indication of how much compression is achieved for a particular image. The compression ratio typically affects the picture quality. The tradeoff between compression ratio and picture quality is an important one to consider when compressing images [2].

2. 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.

2.1 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 [3]. 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 N1 and N2, and the number of all pixels as N = N1 x N2.
Then, the amount of bits of the original image is N x 8.
Number of pixels = N = N1 x N2
Number of bit = N x 8
Encrypted data = permuted pixel-sequence

Original data =

1	2	3	4	5	6	7	8	9	10

N = 10 Permutation order

13	14	12	68	59	100	111	42	39	36

8, 7, 3, 1, 6, 2, 9, 4, 10, 5

Encrypted data =

1	2	3	4	5	6	7	8	9	10
42	111	12	13	100	14	39	68	36	59

2.2 Compression of Encrypted Image
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 [4].

2.2.1 Advantages of Lossy Compression
1) In some cases a lossy method can produce a much smaller compressed file than any known lossless method.
2) Lossy methods are most often used for compressing sound, images or videos [5].

2.2.2 Steps for Compression of Encrypted Image

1) The network provider divides Permuted pixel sequence, into two parts: the first part made up of (α. N) pixels and the second one containing the rest of the (1 - α) .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.

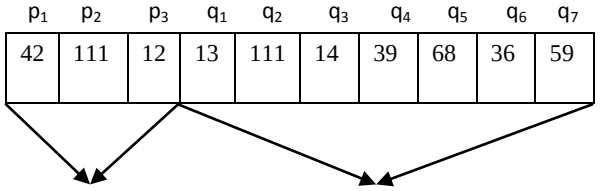
2) Pixels in first part as p_1,p_2,p_3……..$p_{(\alpha.\ N)}$ and pixels in second part as q_1,q_2……$q_{(1\ -\ \alpha\ ).\ N}$. The value of α is within (0, 1).

Where α within (0, 1)

Here consider α = 0.3

N = 10

Encrypted data =



Rigid pixels elastic pixels

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

Q_1, Q_2…… $Q_{(1\ -\ \alpha).\ N}$

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

Here,

H is a public orthogonal matrix with a size of (1 - α). N x (1 - α). N and it can be generated from orthogonal zing a random matrix.

Size of H = (1 - α). N x (1 - α). N

$$H = \begin{pmatrix} 0&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0 \end{pmatrix}$$

Then elastic pixels x H =

Q = [14 59 39 36 100 68 13]

4) For each coefficient Q, calculate

$$Sk = mod\left[round\left(\frac{Qk}{\frac{\Delta}{M}}\right), M\right]$$

k = 1, 2 … (1 - α). N

Where Δ and M are system parameters

The round operation returns the nearest integer and the mod operation gets the remainder. Qk is converted into an integer Sk within [0, M -1].

5) Then $Qk = rk.\Delta + Sk.\left(\frac{\Delta}{M}\right) + Sk$

where rk is rough information & tk is fine information.

The rough information rk and the fine information tk are discarded. While only the information Sk on the medium level remains. The rough information rk will be retrieved by an iterative image reconstruction procedure, and the loss of the fine information tk cannot seriously affect the quality of the reconstructed image,

where

$0 \le Sk \le M - 1$

$$-\frac{\Delta}{2M} \le tk < \frac{\Delta}{2M}$$

e.g. M = 4, Δ = 50

Q = [14 59 39 36 100 68 13]

$$S1 = mod\left[round\left(\frac{Q1}{\frac{\Delta}{M}}\right), M\right] = mod\left[round\left(\frac{14}{\frac{50}{4}}\right), 4\right]$$

$= 1$

$$S3 = mod\left[round\left(\frac{Q3}{\frac{\Delta}{M}}\right), M\right] = mod\left[round\left(\frac{39}{\frac{50}{4}}\right), 4\right]$$

$= 3$

Thus

Sk = [1 1 3 3 0 1 1]

6) Segment The set of Sk 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. Log_2 M]

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

L = (1 - α). N .Log_2 M

Then

L = (1 – 0.3). 10. Log_2 4 = 14

Each value of Sk is represented by Log_2 M bits

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

$$R = \alpha + \left(\frac{Log2M}{8}\right).(1 - \alpha)$$

2.3 Image Reconstruction

In this system, iterative reconstruction is used. Iterative reconstruction refers to iterative algorithms used to reconstruct 2D and 3D images in certain imaging techniques. The advantages of the iterative approach include 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, then in this priory information can be incorporated at each step of the reconstruction process. A receiver can perform the following steps to reconstruct the principal content of the original image.

2.3.1 Steps for Image Reconstruction

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

Sk = [1 1 3 3 0 1 1]

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.
e.g., rigid pixels in encrypted data

1 2 3 4 5 6 7 8 9 10

Permutation order 8, 7, 3, 1, 6, 2, 9, 4, 10

1 2 3 4 5 6 7 8 9 10

		12				111	42		

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 Sk.
Estimate the values for elastic pixels

1 2 3 4 5 6 7 8 9 10

12	12	12	12	62	111	111	42	42	42

Average of 12 and 111

Value of nearest rigid pixel

4) Rearrange the estimated values of elastic pixels using the same permutation way, and denote them as
q′1 q′2 ..... q′(1 - α). N
Rearrange the elastic pixels using the permutation

1 2 3 4 5 6 7 8 9 10

12	12	12	12	62	111	111	42	42	42

Permutation order 8, 7, 3, 1, 6, 2, 9, 4, 10

p_1 p_2 p_3 q'_1 q'_2 q'_3 q'_4 q'_5 q'_6 q'_7

5) Calculate the coefficients
$[Q'_1, Q'_2 \ldots\ldots\ldots Q'_{(1-\alpha).N}] = [q'_1 \; q'_2 \ldots\ldots\ldots q'_{(1-\alpha).N}] . H$
Q’ = [12 62 42 42 111 12 12]
6) Calculate the differences

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

k = 1,2,…….. (1 - α). N

e.g. α = 0.3
M = 4
Δ = 50
Q’ = [12 62 42 42 111 12 12]
Sk = [1 1 3 3 0 1 1]

$$d1 = mod\left[\left(\frac{Q'k}{\frac{\Delta}{M}}\right), M\right] - Sk = mod\left[\left(\frac{12}{\frac{50}{4}}\right), 4\right] - 1$$

$$= -0.04$$

$$d5 = mod\left[\left(\frac{Q'k}{\frac{\Delta}{M}}\right), M\right] - Sk = mod\left[\left(\frac{111}{\frac{50}{4}}\right), 4\right] - 0$$

$$= 0.08$$

Then total dk
dk = [-0.04 - 0.04 0.36 0.36 0.88 -0.04 - 0.04]
7) Modify the coefficients to the closest values consistent with the corresponding Sk.

$$Q''k = \begin{cases} \left[\left(\frac{Q'k}{\Delta}\right) + 1\right].\Delta + Sk.\frac{\Delta}{M} \ldots\ldots if dk \geq \frac{M}{2} \\ \left[\left(\frac{Q'k}{\Delta}\right)\right].\Delta + Sk.\frac{\Delta}{M} \ldots\ldots if -\frac{M}{2} \leq dk < \frac{M}{2} \\ \left[\left(\frac{Q'k}{\Delta}\right) - 1\right].\Delta + Sk.\frac{\Delta}{M} \ldots\ldots if dk < -\frac{M}{2} \end{cases}$$

e.g. Q’ = [12 62 42 42 111 12 12]
S_k = [1 1 3 3 0 1 1]
dk = [-0.04 - 0.04 0.36 0.36 0.88 -0.04 - 0.04]
$\frac{M}{2} = 2$
Δ = 50
$-2 \leq d_k < 2$

$$Q''1 = \left(\frac{12}{50}\right).50 + 1.\frac{50}{4} = 12.$$

Q’’ = [12.5 62.5 37.5 37.5 100 12.5 12.5]
8) Perform inverse transform

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

q’’ = [12.5 100 12.5 37.5 12.5 37.5 62.5]
9) Calculate the average energy of difference between the two versions of elastic pixels

42	111	12	12	111	12	42	12	42	62

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

1 If D is greater than a threshold T (recommended 0.05), go back to step 5 – iterating

2 Otherwise, terminate the iteration and output the image made up of the rigid pixels and the final version of elastic pixels

e.g q' = [12 111 12 42 12 42 62]

q'' = [12.5 100 12.5 37.5 12.5 37.5 62.5]

D =23.21 ≥ 0.05

go back to step 5.

3. SYSTEM DESIGN

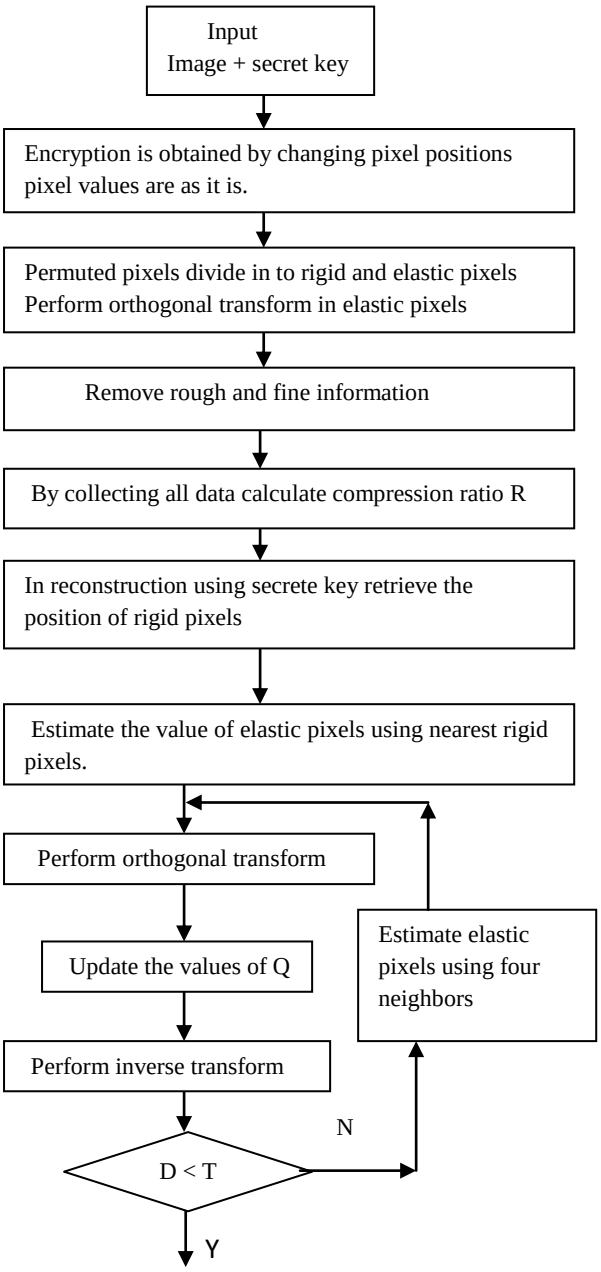


Fig-1 Total procedure with Flowchart

1. Then encrypt image using pseudo random permutation. In this method the pixel values are same after encryption but their position will be changed. The image obtained is nearly similar to the original image due to high correlation between the adjacent pixels.
2. Then compression of encrypted images, 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.
3. After encryption and compression, reconstruction of original image takes place. In which, 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.
4. 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.
5. Calculate the coefficients using orthogonal transform.
6. Modify the coefficients to the closest values consistent with the corresponding Sk.
7. Perform inverse transform.
8. Calculate the average energy of difference between the two versions of elastic pixels.
9. a) If D is greater than a threshold T (recommended 0.05), go back to step 5 - iterating
   b) Otherwise, terminate the iteration and output the image made up of the rigid pixels and the final version of elastic pixels.

4. RESULT

The image Lena used as the original image.

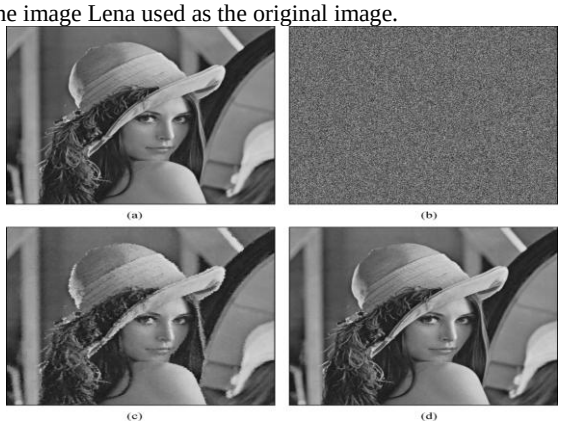


Fig-2 (a) Original image Lena, (b) its encrypted version, (c) the medium reconstructed image from compressed data with less PSNR, and (d) the final reconstructed image with more PSNR

Table-1 Compression ratio R and PSNR (dB) in reconstructed image with different parameters for test image Lena

		α = 0.15	α = 0.10
M = 8	Δ =80	0.47,39.6	0.44,39.4
M = 8	Δ =60	0.47,42.1	0.44,41.9
M = 8	Δ =50	0.47,43.7	0.44,43.5
M = 6	Δ =80	0.42,37.1	0.39,36.9
M = 6	Δ =60	0.42,39.6	0.39,39.4
M = 6	Δ =50	0.42,41.2	0.39,40.9
M = 4	Δ =80	0.36,33.6	0.33,33.4
M = 4	Δ =60	0.36,36.1	0.33,35.9
M = 4	Δ =50	0.36,37.7	0.33,37.4

5. CONCLUSION

This work proposed a novel idea for compressing and encrypted image and designed a practical scheme made up of image encryption, lossy compression, and iterative reconstruction. The original image is encrypted by pseudorandom permutation, and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. When having the compressed data and the permutation way, an iterative updating procedure is used to retrieve the values of coefficients by exploiting spatial correlation in natural image, leading to a 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. In the encryption phase of the proposed system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data.

6. REFRENCES

[1] Mitra, Y. V. Subba Rao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques"

[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] Daniel Schonberg, Stark C. Draper, Chuohao Yeo, Kannan Ramchandran, "Towards Compression of Encrypted Images and Video Sequences"

[4] Ibrahim Fathy El-Ashry, "Digital Image Encryption" A Thesis Submitted for The Degree of M. Sc. of Communications Engineering**.**

[5] D. Schonberg, S. C. Draper, C. Yeo, K. Ramchandran, "Toward compression of encrypted images and video sequences" IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.

AUTHOR'S PROFILE

Asha Pandit Ghodake received her B.E. degree in Electronics Engineering 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, 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 Engineering from Shivaji University, Kolhapur, Maharashtra in 1998 and M.E. from BATU, Lonere in year 2005. Currently she is 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.