Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique

Pooja Mishra[1], Biju Thankachan[2]

[12]Disha Institute of Management and Technology, Chhattisgarh Swami Vivekanand Technical University
Raipur, Chhattisgarh India

Abstract: ***In present times, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption. There are so many different techniques should be used to protect confidential image data from an unauthorized access. In this paper, we are using multi encryption technique. Here we are using more than one encryption algorithm. First we apply segmentation process to divide the image in to 2n equal parts. These image parts are encrypted through encryption algorithm. In encryption for each image part we are using different encryption key. Now we add n bits to each image parts to identify it uniquely. Encryption keys are depends on additional bits. After encryption we are sending image parts through the network. At the receiver side first we extract the additional bits then we apply decryption algorithm into the image parts with the help of appropriate decryption key.***

Keywords*:* Encryption, Decryption, Image parts, Segmentation, Key

1. Introduction

The most ancient and basic problem of cryptography is secure communication over an insecure channel. Party A wants to send to party B a secret message over a communication line, which may be tapped by an adversary. The development of information technology and the rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted in open networks such as the internet [1]. Each type of data has its own aspects, and different techniques should be used to protect confidential image data from unauthorized access [2]. Encryption is the process of transforming the information to ensure its security [3].The recent advances in technology, especially in computer industry and communications, allowed potentially gigantic market for distributing digital multimedia content through the Internet. However, the proliferation of digital documents, image processing tools, and the worldwide availability of Internet access has created an ideal medium for copyright fraud and uncontrollable distribution of multimedia such as image, text, audio, and video content [4]. Another major challenge now is how to protect the intellectual property of multimedia content in multimedia networks.

To deal with the technical challenges, the two major image security technologies are under use: (a) Image encryption techniques to provide end-to-end security when distributing digital content over a variety of distributions systems, and (b) Watermarking techniques as a tool to achieve copyright protection, ownership trace, and authentication. In this paper, the current research efforts in image encryption techniques based on chaotic schemes are discussed.

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding.

Images are different from texts in many aspects such as high correlation among pixels and high redundancy. Thus, a variety of new image encryption schemes have been proposed [5]. Although we may use the traditional encryption algorithms to encrypt images directly, it is not a good idea for two reasons. The first is the image size is often larger than text. Consequently, the traditional encryption algorithms need longer time to directly encrypt the image data, the second, is the decrypted text must be equal to the original text, but this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [6], [7] - [9]. According to [10] image encryption techniques try to convert an image to another one that is hard to understand. On the other side, image decryption retrieves the original image from the encrypted one. Most of these proposed algorithms concentrate on dividing the image into different blocks which result in a stronger encryption algorithm with less correlation between the shares[11]. According to [12] proposes a new image encryption based on random pixel permutation with the motivation to maintain the quality of the image. The values used in the encryption process are preserved in the form of a 64 bit key and sent to the receivers. The receivers jointly use the key and the shares to see the secret.

2. Methodology

2.1 Encryption Process

Step 1: Input Image- The image encryption process first selects a random image of n*n size. .An image can be RGB color image or GRAY scale image.

Step 2: Segmentation-Image is divided in to 2^n parts. Here I is an image and divided in to 2^2 parts I1, I2, I3 and I4 as shown in figure 2.

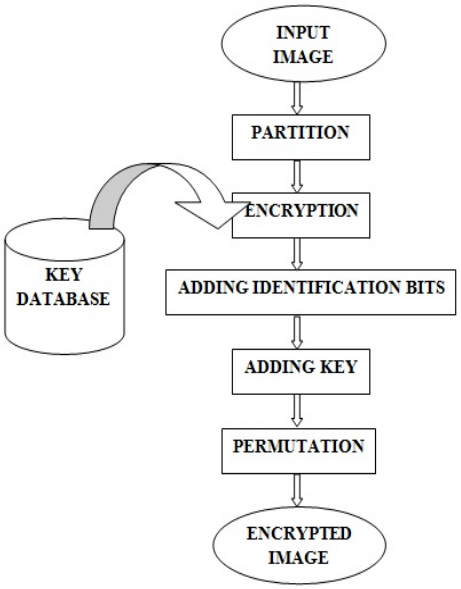

Figure 1: Encryption Process

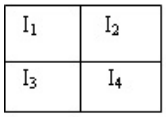

Figure 2: Image segmentation

Step 3: Encryption- Image encryption technique try to convert original image to another image that is hard to understand, to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Here image is encrypted with encryption algorithm. For each image parts we are using different keys to ensure security.

I1' = E (K1, I1)
I2' = E (K2, I2)
I3' = E (K3, I3)
I4' = E (K4, I4)

Where, E is an encryption algorithm. K1, K2, K3 and K4 are keys.I1 , I2 , I3 and I4 are original image parts and I1' , I2' , I3' and I4' are encrypted image parts respectively.

Step 4: Adding additional bits - There are more than one parts of image, to uniquely identify each part we are adding extra bits at the end of the each image part. This extra bit represents the sequence of parts of original image. Image I is divided in to 2n equal parts and we need n bits to identify each part. If image I is divided in to four parts then 2 bits are required for identification.

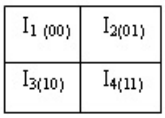

Fig 3: Adding additional bits

Step 5: Adding x bit key - In this step we are adding x bit key at the end of each parts. Now this bit shows gray value of image, so stranger cannot predict it as a key. Each image parts having different keys, this increases security level.

Step 6: Permutation - In this process we are changing the original sequence of image parts. This process will increase the security during transmission.

Step 7: Send the image - Send the image through the network.

2.2 Key Distribution

Key is the very important part of the encryption algorithm. In this algorithm we are adding keys at the end of image. Each image parts having different keys and we are adding respective keys at the end of image. By using this technique keys are converted in to gray values of image so stranger can't extract keys from image.

2.3 Decryption Process

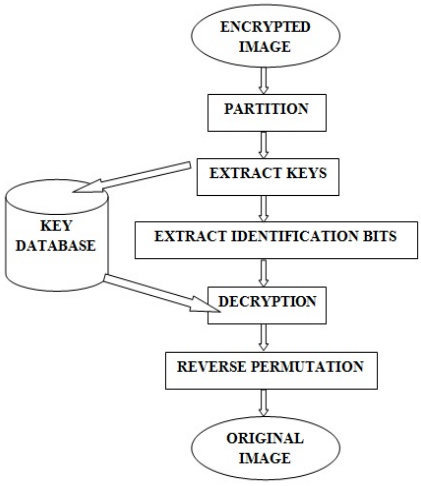

Figure 4: Decryption Process

Step 1: Input Image – Here the input is encrypted image parts. If image I is divided in to four parts I_1, I_2, I_3 and I_4 then its encrypted part is represented as I_1', I_2', I_3' and I_4'. Individual image part is given in to this step.

Step 2: Extracting Keys – In this step we extract the key from the end of the image parts gray values. Each image parts gray values. Each image parts have their respective key.

Step 3: Identifying actual sequence of image parts – In this step we are identifying the actual sequence of image parts to rearrange the image parts. We extract the added bits to identify the original sequence of an image.

Step 4: Decrypt image parts – After identifying the added bits we apply decryption algorithm. Each image parts has their encryption key. We are using this key to decrypt image parts, it increases security level. No one can decrypt the image through the single decryption key.

Step 5: Combine the image – Here we rearrange the image parts with the help of additional bits.

Step 6: Original image – After rearranging we find original image I.

3. Result Analysis

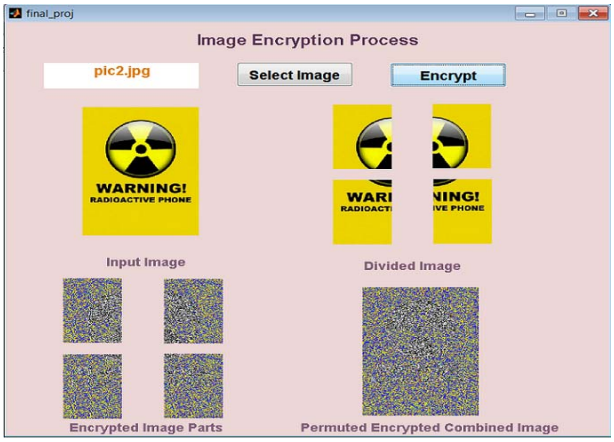

Figure 5: Encryption process

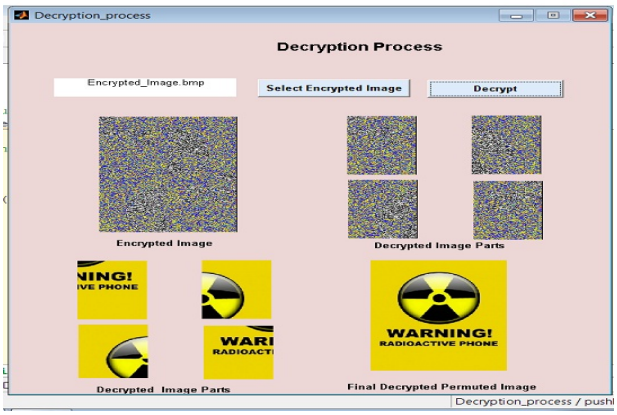

Figure 6: Decryption process

4. Performance Analysis

Performance of encryption algorithm can be analyzed by histogram correlation and entropy as a measure of security [13].

S. No.	Name of Image	Time Analysis		Correlation Analysis		Histogram Analysis
		Encryption Time (sec)	Decryption Time (sec)	Encrypt image Vs. Original image	Decrpt image vs. Original image	Original image vs. Encrypted image
1	Img1	22.22	18.02	0.0054	1	1.9 e+06
2	Img4	18.86	18.01	0.0051	1	4.8 e+06
3	Img5	29.05	21.44	0.0061	1	8.9 e+06
4	Img7	29.37	27.25	0.0043	1	5.5 e+06
5	Img8	20.32	17.99	0.0039	1	3.4 e+06
6	Img9	37.48	27.23	0.0021	1	2.7 e+06
7	Img10	20.4	18	0.0019	1	1.4 e+06
8	Img11	29.23	27.16	0.0034	1	2.1 e+06
9	Img13	20.37	18.07	0.0011	1	3.1 e+06
10	Img20	20.8	18.03	0.0047	1	4.0 e+07

Table 1.1: Result Analysis

4.1 Histogram Analysis

To prevent the leakage of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies that, how the pixel values of image are distributed. The histogram of original image contains large sharp rises followed by sharp declines. And the histograms of the encrypted images should have uniform distribution which are significantly different from original image and have no statistical similarity in appearance. Therefore, the surveyed algorithm does not provide any clue for statistical attack.

4.2 Correlation Analysis

There is a very good correlation among adjacent pixels in the digital image [14]. Following Equations are used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations: x and y are intensity values of two neighboring pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{--eq (1)}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)^2 \quad \text{--eq (2)}$$

$$cov(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)(y_j - \frac{1}{N}\sum_{j=1}^{N}y_j) \quad \text{--eq (3)}$$

100 pairs of two adjacent pixels are selected randomly from image to test correlation. Neighboring pixels in the plain-image are correlated too much, while there is a little correlation between neighboring pixels in the encrypted image. Correlation among neighboring pixels in encrypted image should be as small as possible for higher security.

4.3 Information Entropy

Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = \sum_{i=0}^{2N-1} P(m_i)\log_2\frac{1}{P(m_i)}. \quad \text{--eq (4)}$$

where $P(mi)$ represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e. m= $\{m_1, m_2, ..., m_2^8\}$. When the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. For higher security entropy should not be smaller than ideal value.

5. Conclusion

There are so many technique to make an image secure. Some of the encryption techniques used selective part of an image for encryption and some others apply encryption algorithm on whole image bit by bit. Use of this multi-encryption technique assures high security of the images. Permutation process moves the security level one step ahead. We can apply this technique in all type of images. This method does not affect the quality of image.

From table 1.1 it can be conclude that correlation between original image and encrypted image is 0.0011 in best case and it is 0.0061 in worst case. It means, in best case purposed method can encrypt images, with 99% efficiency. Histogram analysis shows that histogram of original image and encrypted images are at least 1.9×10^6 different which shows a very good quality of encryption.

References

[1] W. Lee, T. Chen and C. Chieh Lee, “Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology. Vol. 2, no. 2 , 2003, pp. 191- 200.

[2] Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol.1, no. 1, 2006, p.127.

[3] H. El-din H. Ahmed, M. K Hamdy, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Optical Engineering, Vol. 45, Issue 10107003, 2006.

[4] Borko Furht, Daniel Socek, Ahmet M. Eskicioglu, “*Fundamentals of Multimedia Encryption Techniques*”.

[5] K. Wang , Pei , Z. Liuhua ,S. Aiguo Song, H. Zhenya, "On the security of 3D Cat map based symmetric image encryption scheme," Elsevier, Physics Letters A, Vol. 343,Issue 6, 2005, pp. 432–439.

[6] R. m. Syed, "Anew encryption algorithm for high throughput multimedia," IN: Interactive Multimedia Systems, 2002, p. 269.

[7] S. Han, and S. Yang, "An Asymmet ric Image Encrypt ion Based on Mat r ix Trans format ion," e c t I transactions on computer and informa t i on technology vol . 1, no. 2 , 2005 .

[8] D. Salomon, "Data compression, Image compression," Fourt h addit ion, Springer London , 2005, pp. 263-530 .

[9] Ozturk, and I.Sogukpinar, "Analysis and comparison of image encryption algorithm," International Journal of Information Technology, Vol. 1, no. 2, pp. 64-67.

[10] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708,711.

[11] Mohammad Ali Bani Younes and Aman Jantan “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption”, IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.4, April 2008 191.

[12] Sesha Pallavi Indrakanti and P.S.Avadhani “Permutation based Image Encryption Technique” IJCA International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[13] Alireza Jolfaei and Abdolrasoul Mirghadri “Survey: Image Encryption Using Salsa20”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010.

[14] N. Pisarchik and M. Zanin, “Image Encryption with Chaotically Coupled Chaotic Maps,” Physica D, 237, 20, pp. 2638-2648, 2008.

Author Profile

Pooja Mishra received the B.E degree in Computer Science and Engineering from the Chhattisgarh Swami Vivekanad Technical University (CSVTU), Bhilai, India, in 2009, and pursuing her M.Tech. Degree in Information Security in CSVTU, Bhilai , India. Her research interests include cryptography, Image Processing, Parallal Computing.

Biju Thankachan is an Associate Professor in Disha Institute of Management & Technology; Raipur India He is a B. Tech. in Electrical & Electronics Engineering, and M.E in Computer Science & Engineering. His area of interest include Algorithms and Artificial Intelligence and is keenly interested in Human-Computer Interaction and finding solutions to real-life problems using computers.