Highly Secure Method for Image Transmission using Image Segmentation, Permutation and Multi Encryption Technique

Pratibha Pradhan[1] Rasmiranjan Samantray[2]
[1,2]Central College of Engineering and Management, Kabir Nagar, Raipur, 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 same 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, and then we add n bits to each image parts to identify it uniquely. These image parts are encrypted through encryption algorithm. For each image part we are using different encryption key. Encryption key 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, Permutation, Key

I. INTRODUCTION

The most ancient and basic problem of cryptography is secure communication over an insecure channel. Source wants to send to destination 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.

II. METHODOLOGY

A. Encryption Process

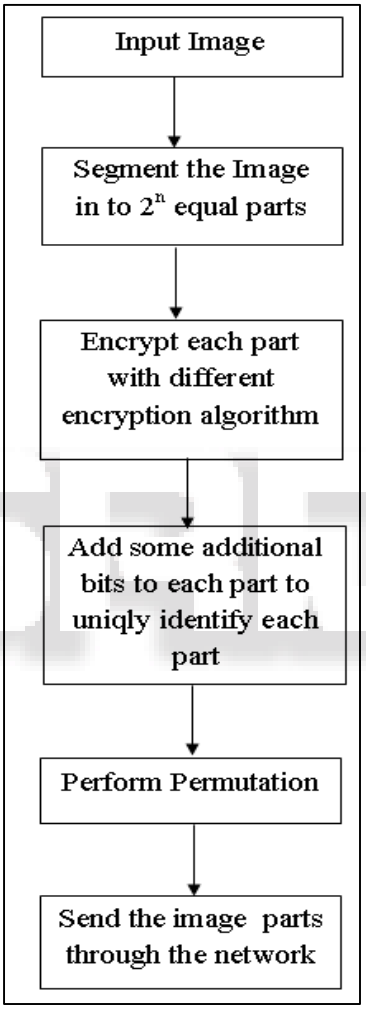

Fig. 1: Encryption Process

1) Step 1: Input Image- An image can be RGB colour image or GRAY scale image.
2) Step 2: Segmentation-Image is divided in to 2^n parts. Here I is an image and divided in to 2^n parts I_1, I_2, I_3 and I_4 as shown in fig 2.

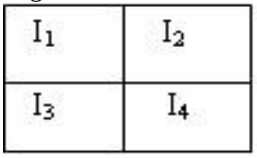

Figure 2: Image segmentation

3) Step 3: Encryption- Image encryption techniques 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 each image part is encrypted with different encryption algorithm and different keys.

$I_1' = E1(K,I_1)$
$I_2' = E2(K,I_2)$
$I_3' = E3(K,I_3)$
$I_4' = E4(K,I_4)$

Where E1, E2, E3, and E4 are different encryption algorithm. I_1, I_3 and I_4 are original image parts and I_1', I_2', I_3' and I_4' are encrypted image parts respectively.

4) Step 4: Adding additional bits - There are more than one parts of image, to uniqly 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 2^n 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.

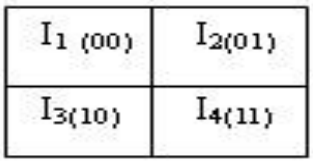

Fig. 3: Adding additional bits

5) Step 5: Permutation - In this process we are changing the actual sequence of image parts. This process will increase the security during transmission.
6) Step 6: Send the image - Send the image through the network.

B. Decryption Process

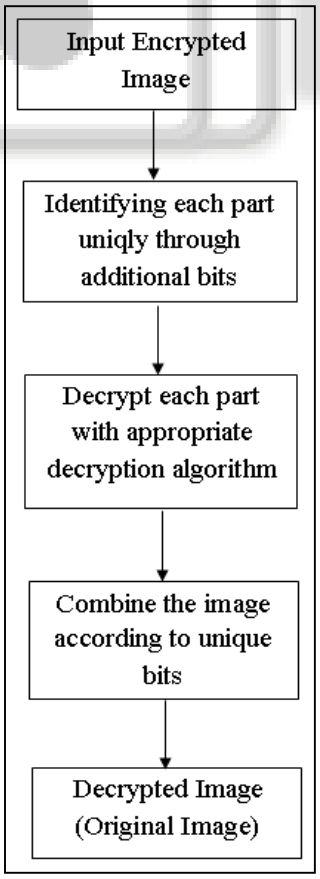

Fig. 4: Decryption process

1) 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.
2) Step 2: Identifying actual sequence of image parts – In this step we are identifying the actual sequence of image parts to rearrange the image parts. Each image part is encrypted with different encryption algorithm. We extract the added bits to identify the appropriate encryption algorithm.
3) Step 3: Decrypt image parts – After identifying the added bits we apply decryption algorithm. Each image parts has different decryption algorithm, it increases security level. No one can decrypt the image through the single decryption algorithm.
4) Step 4: Combine the image – Here we rearrange the image parts with the help of additional bits.
5) Step 5: Original image – After rearranging we find original image I.

III. RESULT ANALYSIS

The evaluation parameters have been described in below section. The proposed image encryption scheme performs adequately in terms of security. The different parameter analysis between original images and encrypted images is shown below.

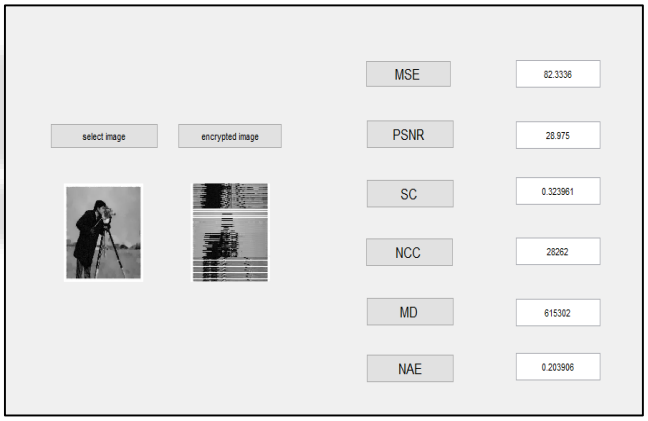

Fig. 5: The different parameter analysis between original images and encrypted images

Fig. 6: The different parameter analysis between encrypted images and decrypted images

NO.	IMAGES	MSE	PSNR	SC	NCC	MD	NAE
1.	Cameraman	82.3336	28.975	0.323961	28262	615302	0.203906
2.	Football	78.1752	29.2001	0.288492	13869	688760	0.366773
3	Lena	98.7221	28.1867	0.333333	22500	446928	0.160128
4	Lily	106.323	27.8645	0.333374	22500	574516	0.160922
5	Rice	89.5198	28.6116	0.333333	22500	242602	0.0598421
6	Rose	89.4864	28.6132	0.333276	22507	548056	0.21711

Table 1: The different parameter analysis between encrypted images and original images shown in below table

NO.	IMAGES	MSE	PSNR	SC	NCC	MD	NAE
1.	Cameraman	47.1483	31.3961	0.328245	35788	277252	0.0919479
2.	Football	58.4258	30.4648	0.285377	89307	434704	0.230145
3	Lena	49.2324	31.2083	0.333333	22500	229411	0.0822068
4	Lily	59.4908	30.3863	0.333292	22506	465186	0.130282
5	Rice	45.6544	31.536	0.333333	22500	129138	0.0314658
6	Rose	32.2708	33.0427	0.333337	22503	141257	0.0559885

Table 2: The different parameter analysis between encrypted images and decrypted images shown in below table

IV. 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 multiencryption 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 and table 2 shows the values of different parameters of different images. It means, in best case purposed method can encrypt images, with 99% efficiency .The Processing time for images is more due to multi encryption technique. The processing time can be reduced. The proposed highly secured method for image transmission. Can be used in military applications.

References

[1] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on rubik's cube principle," Journal of Electrical and Computer Engineering, vol. 2012, p. 7, 2012.
[2] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," Optics and Lasers in Engineering, vol. 88, pp. 197–213, 2017.
[3] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," Multimedia Tools and Applications, vol. 76, no. 1, pp. 1159–1175, 2017.
[4] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on dwt and multichaos mapping," Journal of Sensors, vol. 2016, 2016.
[5] G. Ye, H. Zhao, and H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion," Nonlinear Dynamics, vol. 83, no. 4, pp. 2067–2077, 2016.
[6] Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using dna and chaotic logistic maps," Multimedia Tools and Applications, vol. 75, no. 10, pp. 5455–5472, 2016.
[7] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic s-boxes composed of dna sequences," Multimedia Tools and Applications, vol. 75, no. 8, pp. 4363–4382, 2016.
[8] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," Optics and Lasers in Engineering, vol. 84, pp. 26–36, 2016.[9] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, vol. 78, pp. 17–25, 2016.
[9] J.-C. Yen and J.-I. Guo, "A new chaotic mirror-like image encryption algorithm and its vlsi architecture," vol. 10, no. 2, pp. 236–247, 2000.
[10] F. Belkhouche and U. Qidwai, "Binary image encoding using 1d chaotic maps," in IEEE Region 5, 2003 Annual Technical Conference. IEEE, 2003, pp. 39–43.
[11] Stallings W. "Pseudorandom Numbers "in Cryptography and Network Security- Principles and Practices, 5th edition.
[12] Sivaranjani, K.; Prabahar, P.B. "Mended algorithm for image encryption based on random shuffling technique", Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, on page(s): 1 – 4

