An Image Encryption Technique based on Concatenating Images of Same Dimensions

Mohit Kumar
Research Scholar
Amity University Haryana
India

Akshat Agrawal
Assistant Professor
Amity University Haryana
India

Ankit Garg
Assistant Professor
Amity University Haryana
India

ABSTRACT

Images are widely used in many areas for various purposes. Some images may have confidential information, so security of secrete images is a major issue. Various image encryption algorithms provide security to images. However, traditional encryption techniques encode one image at a time, which leads to weak security in the encrypted image due to small size of the image. In this paper, an image encryption technique is imparted that concatenate four images of the same dimension into one and then produce single encrypted image. In result, encrypted image is more secure due to the large size. This encrypted image has high entropy and low correlation coefficient, so this encrypted image is more difficult to understand compared to four separated images.

General Terms

Image security and image processing

Keywords

Correlation coefficient, concatenation, entropy, histogram and image

1. INTRODUCTION

Multimedia technologies are developing swiftly and it is an effective way to communicate, so users use this technology widely. Images are a part of multimedia and tremendously used in various areas, for example in communication, business, entertainment etc. Some images may be highly confidential; they need security so that confidentiality can be maintained. Encryption is an effective way to provide protection from illegal access [1, 2, 3]. Many image encryption techniques provide security to images. The main issue is to confirm the capability of an image encryption technique. So, diverse parameters are used to measure the capability of an image encryption algorithm by analyzing the encrypted image. Entropy and correlation coefficient are two critical parameters to measure the security level and capability of a technique.

Entropy calculates the degree of randomness and uniform distribution in the system [4, 5]. Thus, an encryption technique should show uncertainty and uniform distribution in the encryption procedure [5]. Information entropy is calculated by the equation (1) [5, 6].

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2\left[P(m_i)\right] \qquad (1)$$

Where p (m_i) defines the probability of a pixel and N is the number of bits in each pixel [5]. For a gray level image, each pixel has 8 bits, so the probability of a pixel is $1/2^8$ [5]. Hence, information entropy of the gray level image is H (m) = 8 [5]. However, practically it is intricate to obtain ideal entropy; so slight difference is also tolerable [5].

Correlation coefficient assesses the correlation between two adjoining pixels in an image [5, 6, 7]. Generally, correlation measures the degree of similarity between two pixels. An encrypted image should have low correlation between two adjoining pixels [5, 6, 7], so that it becomes difficult to guess the value of neighbors of a pixel. For example, xi and yi are two pixel pair then the correlation coefficient can be obtained by the equation (5) [5, 6, 7].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\ , \qquad (2)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \qquad (3)$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\ (y_i - E(y))\ , \qquad (4)$$

$$r_{xy} = \frac{\operatorname{cov(x,y)}}{\sqrt{D(x)}\sqrt{D(y)}}\ , \qquad (5)$$

$$\text{where } \sqrt{\mathrm{D(x)}} \neq 0 \text{ and } \sqrt{\mathrm{D(y)}} \neq 0$$

Where xi and yi are gray level value of two adjacent pixels, N is the number of pairs (xi, yi) and E(x) is the mean of xi and E(y) is the mean of yi [5, 6].

In experiments, it is observed that correlation coefficient and entropy in an encrypted image depend on the area of the image [8]. Encrypted images of large area have a more reduced correlation coefficient as compared to images of less area [8]. Moreover, encrypted images of large region have more entropy compared to images of less area [8]. An image encryption algorithm can take the benefit of this concept.

In this paper, a technique is proposed that joins four images of the same dimension and produce a single encrypted image. This encrypted image has more entropy and low correlation coefficient, so this encrypted image is more secure than four different encrypted images.

Rest of paper has the following section: proposed technique, decryption, experiment and results, conclusion and future work.

2. PROPOSED TECHNIQUE

Proposed technique works in two main phases; joining phase and encryption phase.

In joining phase, imparted technique takes four different images of same dimension and joins them to make a single image. This single image is provided to second phase for encryption. Figure 1 shows the block diagram of this technique.

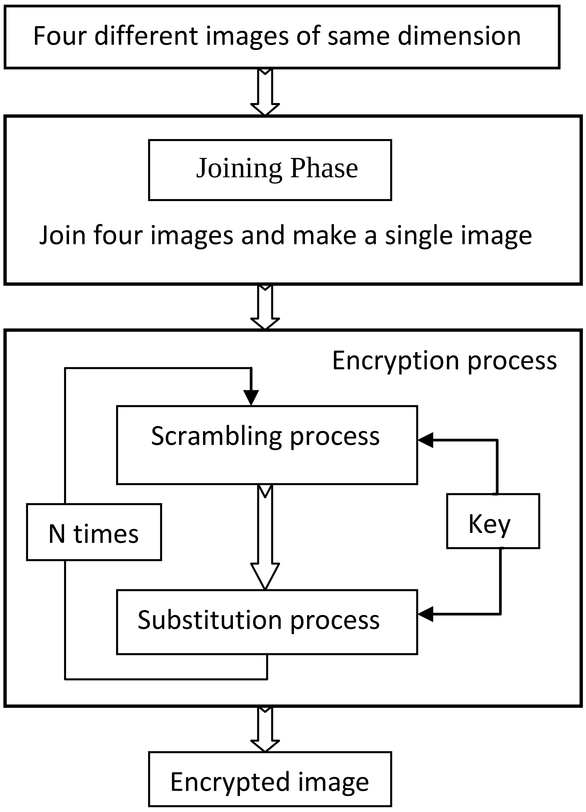

Fig 1. Block diagram of proposed technique

2.1 Joining Phase

In this phase, take four images of the same dimension and join them in the form of a grid. In result, a single image is generated which enters in the encryption phase.

2.2 Encryption phase

Encryption process further works in two stages: scrambling and substitution, which are following as

2.2.1 Scrambling

Step 1: apply swapping operation among rows with the help of key.

Step 2: apply swapping operation among columns with the help of key.

Step 3: apply circular rotation on all rows with the help of key.

Step 4: apply circular rotation on all columns with the help of key.

Step 5: end of scrambling process.

Step 6: A scrambled image is produced and this image will enter in substitution phase.

2.2.2 Substitution

This phase has following steps

Step 1: transform image matrix to one-dimensional array.

Step 2: pick 50 pixels in sequence and convert into bits.

Step 3: operate the XOR function on these bits with a key of 400 bits.

Step 4: operate a circular shift process on the result of step 3 with the help of key.

Step 5: obtain the complement of key

Step 6: operate again XOR function on the result of step 4 and the complement of key.

Step 7: decompose the resulting 400 bits of step 6 into 50 segments, where each segment will have 8 bits.

Step 8: convert each segment to equivalent decimal number. These decimal numbers are encrypted pixels.

Step 9: replace these encrypted pixels with the pixels in one-dimensional array.

Step 10: pick next 50 pixels and repeat step from 3 to 9.

Step 11: if 50 pixels are not available for encryption in the end, then pick the rest pixels and repeat step from 3 to 9. But this time key will have the number of bits that will be equal to number of rest pixels multiplied by 8.

Step 12: convert one-dimensional array into two-dimensional matrix having the same dimension as the original image.

Step 13 end of substitution process. The resultant matrix is encrypted image.

3. DECRYPTION

In order to decrypt the received image, the decoding process is applied that is reverse procedure of the encryption. In decryption, substitution takes place, followed by scrambling. Thus, a decrypted image is generated that is still has four different images. The last step is to split the four images by decomposing into four equal parts. To separate the decrypted image into the four equal pieces, find out the size of this image then decompose from middle horizontally. Thus, two disconnected parts are obtained; afterward, decompose from the middle to both parts vertically. Consequently, receiver will obtain four detached images without any loss of information and confidentiality.

4. EXPERIMENT AND RESULT

For this experiment, the four different images of same dimension have been taken that are represented by figure 2, figure 3, figure 4 and figure 5.

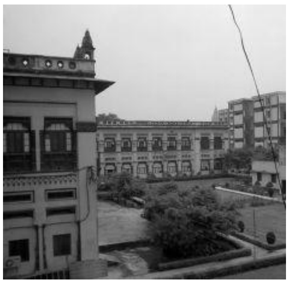

Fig 2. First image

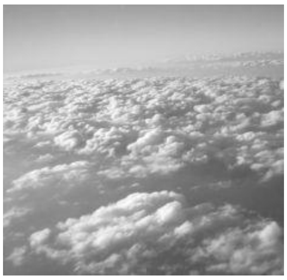

Fig 3. Second image

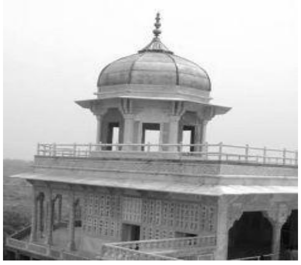

Fig 4. Third image

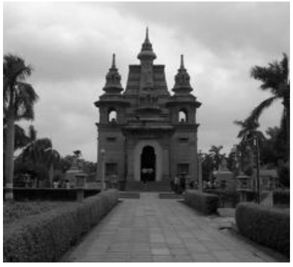

Fig 5. Fourth image

Figure 6 represents the concatenated image; figure 7 illustrates the histogram of concatenated image, figure 8 shows the encrypted image of the combined image and figure 9 represents the histogram of this encrypted image.

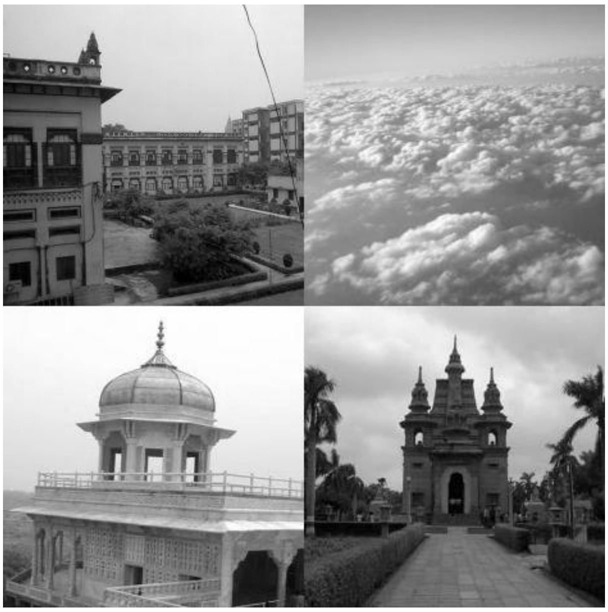

Fig 6. Concatenated image

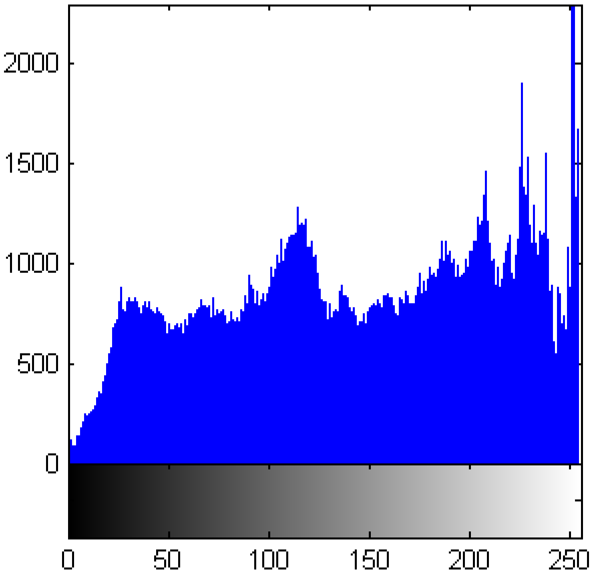

Fig 7. Histogram of concatenated image

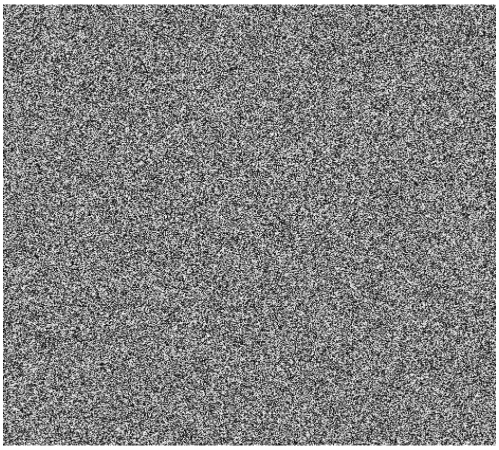

Fig 8. Encrypted image of concatenated image

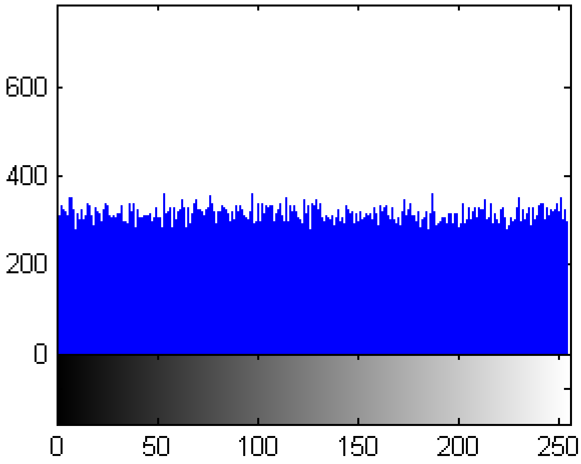

Fig 9. Histogram of encrypted image

After receiving this encrypted image, a user applies decryption process to decrypt it and afterward decomposes this concatenated image into two halves. Figure 10 illustrate decrypted image, figure 11 and figure 12 shows two halves.

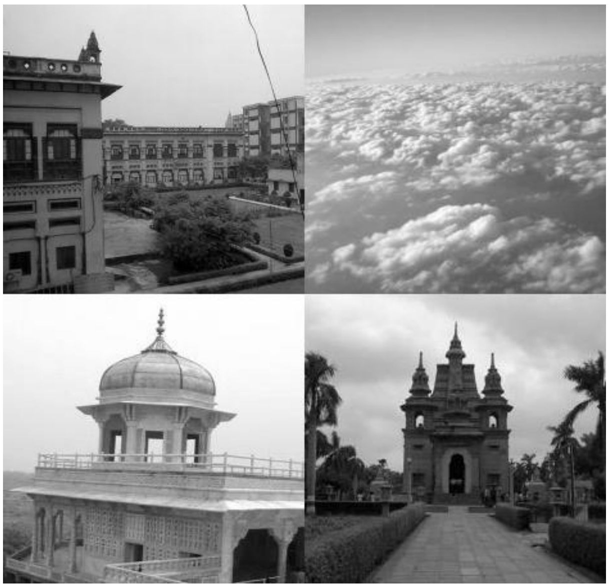

Fig 10. Decrypted image

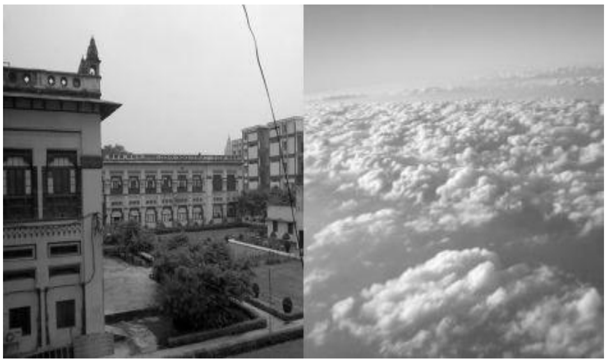

Fig 11. First half

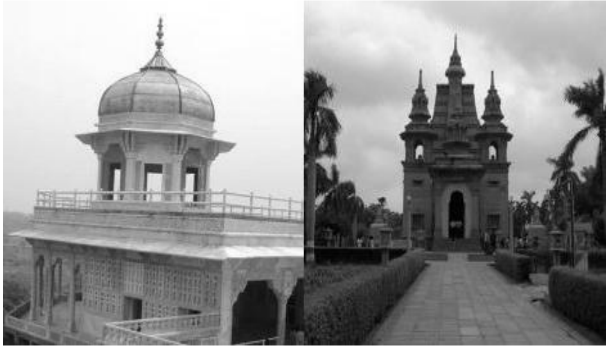

Fig 12. Second half

After decomposing into two halves, a user further applies decomposition on these halves and obtains four separated image. Figure 13, figure 14, figure 15 and figure 16 shows detached images.

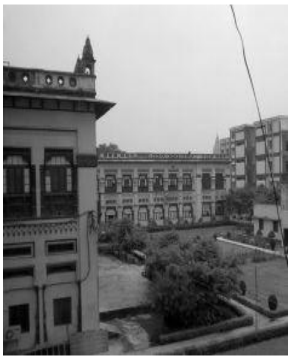

Fig 13. Decrypted image 1

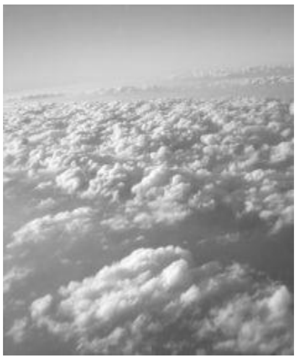

Fig 14. Decrypted image 2

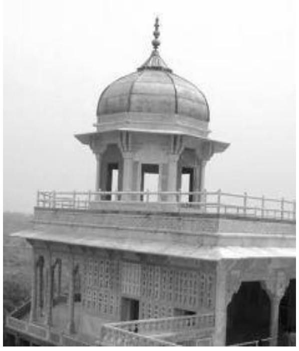

Fig 15. Decrypted image 3

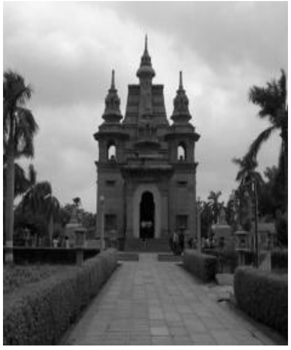

Fig 16. Decrypted image 4

Table 1 has the data of this experiment. It includes entropy and correlation coefficient in individual image and in concatenated image prior to encryption and after the encryption.

Table I. Experimental data

Entropy			Correlation coefficient	
Image (size)	In original image	In encrypted image	In original image	In encrypted image
First image (235*235)	7.4738	7.992	.7080	.0042
Second image (235*235)	7.1468	7.992	.4762	.0045
Third image (235*235)	7.1301	7.991	.7083	.0042
Fourth image (235*235)	7.6207	7.992	.6464	.0047
Concatenated image (470*470)	**7.8701**	**7.9994**	**.4767**	**.0019**

Figure 17 shows the correlation coefficient in encrypted image. In this figure, horizontal or x-axis represents the images. At x-axis number 1 represents the first image, number 2 illustrates the second image, number 3 shows the third image, number 4 shows the fourth image and number 5 represents the concatenated image. In this figure, vertical or y-axis represents the correlation coefficients in encrypted image. This figure confirms that image of large area has lower correlation coefficient than image of small area.

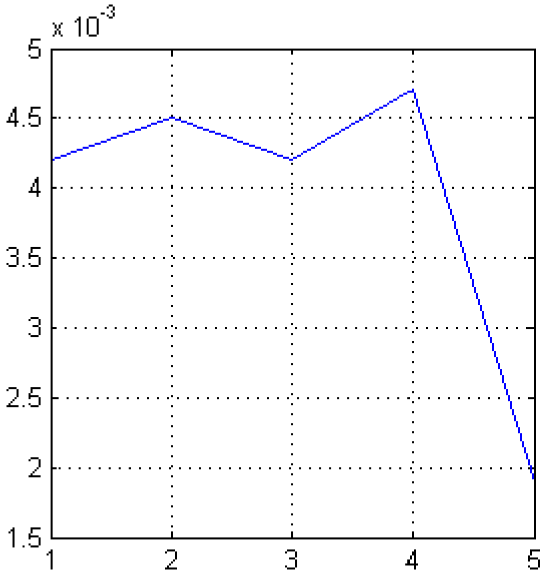

Fig 17. Correlation coefficient in encrypted image

Figure 18 represents the entropy in individual encrypted image and in the concatenated image. In this figure, horizontal or x-axis represents the encrypted image of the first image, second image, third image, fourth image and attached image.

Moreover, vertical or y-axis represents the entropy in the corresponding image. This figure shows that the first image, second image, third image and the fourth image has low entropy due to lower size, the fifth image that is concatenated image has higher entropy. In results, this technique provides high uncertainty in system, which provides high security.

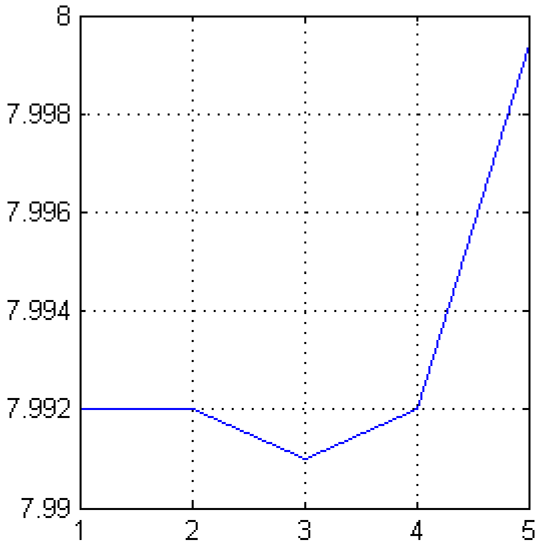

Fig 18. Entropy in encrypted image

5. CONCLUSION

This work reveals that an image of large dimension has a more entropy compared to an image of a small dimension. High entropy provides high randomness and uncertainty in the system. Moreover, after encryption, a large image has low correlation coefficient compared to an image of small size. As, low correlation creates difficulty to guess the value of neighbor pixels so encrypted image is secured. Consequently, this research concludes that a user should encrypt image after concatenating them for higher security, provided that the user want to send multiple images of the same size.

6. FUTURE WORK

As the condition is that dimensions of images should be same to concatenate them, if images are not of the same dimension then a sender can add extra bits in the smaller image to make this image equal to other images.

A video is made up of multiple frames or images with little differences and these frames have same dimensions. So, a user can use this technique effectively in video encryption. To make this technique suitable for videos, there is a need to improve performance of this technique in terms of encryption time. So that it will become usable for real time encryption system.

7. ACKNOWLEDGEMENT

Author is thankful to his guides Mr. Akshat Agrawal and Mr. Ankit Garg who give him an opportunity to carry out this work. Author is also thankful to NPTEL which provides E-learning through online Web and Video courses in Engineering, Science and humanities streams.

8. REFERENCES

[1] W. Stallings, Cryptography and Network Security principles and practices, 3rd ed., Pearson Education, 2003.

[2] H. EI-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

[3] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar "Image Encryption Using Affine Transform and XOR Operation" 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[4] Shujiang Xu, Yinglong Wang, Jizhi Wang, Yucui Guo, "A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map", 2010 2nd International Conference on Signal Processing Systems (ICSPS), 5-7 July 2010, pages: v2-326-v2-330.

[5] Mohit Kumar, Akshat Aggarwal and Ankit Garg, "A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications, Volume-96, no-13, 17 June, 2014, pages:19-26.

[6] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Volume 2012 (2012), Article ID 173931, 13 pages.

[7] Shujiang Xu, Yinglong Wang, Jizhi Wang, Yucui Guo, "A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map", 2010 2nd International Conference on Signal Processing Systems (ICSPS), 5-7 July 2010, pages: v2-326-v2-330.