Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image

Mohit Kumar
Research Scholar
Amity University Haryana
India

Anju Chahal
Research Scholar
Amity University Haryana
India

ABSTRACT

Images have a significant role in communication, entertainment and business etc. Images may convey confidential information, so various image encryption algorithms ensure security of secret images. The correlation coefficient in encrypted image is an important security criterion to measure the level of security of encrypted image. Various factors can affect the correlation coefficient in the encoded image. So, this work reveals the effect of image encryption method and the size of an image on correlation coefficient in the corresponding encrypted image.

General Terms

Data Security, image encryption, image processing.

Keywords

Cipher, correlation coefficient, encryption, encrypted image, image, size of an image

1. INTRODUCTION

The Internet and information technology are growing rapidly so users prefer to communicate through multimedia. Images are highly utilized in communication. Some images convey secret information, so there is always a need to protect these images from illegal access. There are various techniques to making an image secure, for example stenography, cryptography and watermarking etc. Encryption method is a part of cryptography and greatly used to make an image secure [1, 2, and 3]. There are various image encryption algorithms to provide protection to images. So, different criteria are used to measure the capability of an image encryption algorithm and security level of encrypted image. One significant criterion is the correlation coefficient that is used for statistical analysis of encrypted image [4].

Correlation coefficient assesses the correlation between two adjoining pixels in an image [4, 5]. Generally, correlation measures the degree of similarity between two pixels. An encrypted image should have low correlation between two adjoining pixels [4, 5, 6], 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 (4) [4, 5, 6].

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

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

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\,(y_i - E(y)) \ , \qquad (3)$$

$$r_{xy} = \frac{\operatorname{cov(x,y)}}{\sqrt{D(x)}\sqrt{D(y)}} \ , \qquad (4)$$

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

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.

This paper demonstrates the effect of image encryption algorithm and size of an image on correlation coefficient in the corresponding encrypted image. For the demonstration, four different algorithms are used to encrypt a same image of different sizes.

The rest of the paper is divided as: existing algorithms that will be used for experiment, experimental results, conclusion and suggested future work.

2. EXISTING ALGORITHMS

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [3] have suggested a technique that uses 64 bits key in the encryption process. This approach uses the affine transformation to shuffle the pixels by applying four sub keys of 8 bits. Thereafter, this algorithm decomposes an image into 2*2 pixel block size, afterward, applies an XOR operation on each block to change the pixels value.

Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue [7] have imparted a one-dimensional random scrambling based method. At the beginning, this technique transforms a two-dimensional image into the one-dimensional vector and then applies the one-dimensional random scrambling [7]. Thereafter, this algorithm performs an anti transformation on the dispersed vector to generate an encoded image.

Mohammed Abbas and Fadhil Al-Husainy [8] have propounded an approach that relies on the bit level permutation. This technique utilizes two Boolean operations: XOR and Rotation on the bits of the pixels to satisfy the confusion and diffusion properties.

Long Bao and Yicong Zhou have [9] recommended a new chaotic system that constitutes the three distinct one-dimensional chaotic maps. The imparted method utilizes the substitution-permutation network (SPN) structure to obtain the confusion and diffusion property [9, 10].

3. EXPERIMENTAL RESULTS

Four different techniques have been used to observe the impact of size of an image on correlation coefficient in encoded image. For this test, same gray level images of 8 different sizes have been used. The gray level image is shown in figure 1.

Table 1 shows the result of the four different techniques that have been applied on these images. Furthermore, correlation coefficient is calculated in the corresponding encrypted images that are produced after 11 rounds of encryption technique.

Fig 1: Gray image

Table 1. Impact of a technique and size of an image on correlation coefficient in corresponding encrypted image

Size of image (KB)	Four different techniques			
	affine transformation and XOR operation [3]	one-dimensional random scrambling [4]	XOR operation and rotation [5]	Three distinct one-dimensional chaotic map [7]
18	.78591	.10588	.00520	.00837
37	.86584	.11142	.00317	.00615
86	.86593	.10773	.00281	.00527
147	.84580	.09963	.00210	.00345
240	.83011	.09803	.00157	.00267
351	.85119	.09982	.00131	.00182
468	.90243	.09992	.00121	.00152
768	.87217	.097570	.00087	.00093

Figure 2, figure 3, figure 4 and figure 5 illustrate that how the correlation coefficient varies according to size of an image. In these figures, horizontal or x-axis depicts the size of the images in kilo-byte and vertical or y-axis represents the correlation coefficient in the encrypted image. Furthermore, the figure 2 demonstrates the outcome of the algorithm that is based on the affine transformation and the XOR operation. Figure 3 represents the results of the technique that uses one-dimensional random scrambling. Moreover, figure 4 shows the outcome of the approach that applies the XOR operation and rotation. Figure 5 represents the results of the technique that utilizes three distinct one-dimensional chaotic maps.

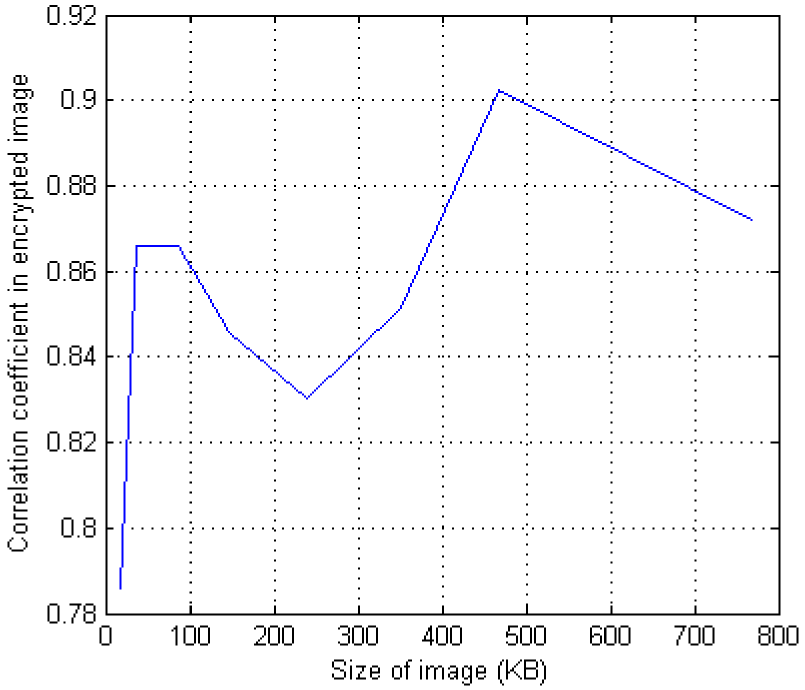

Fig 2: Result of the technique that is based on the affine transformation and the XOR operation

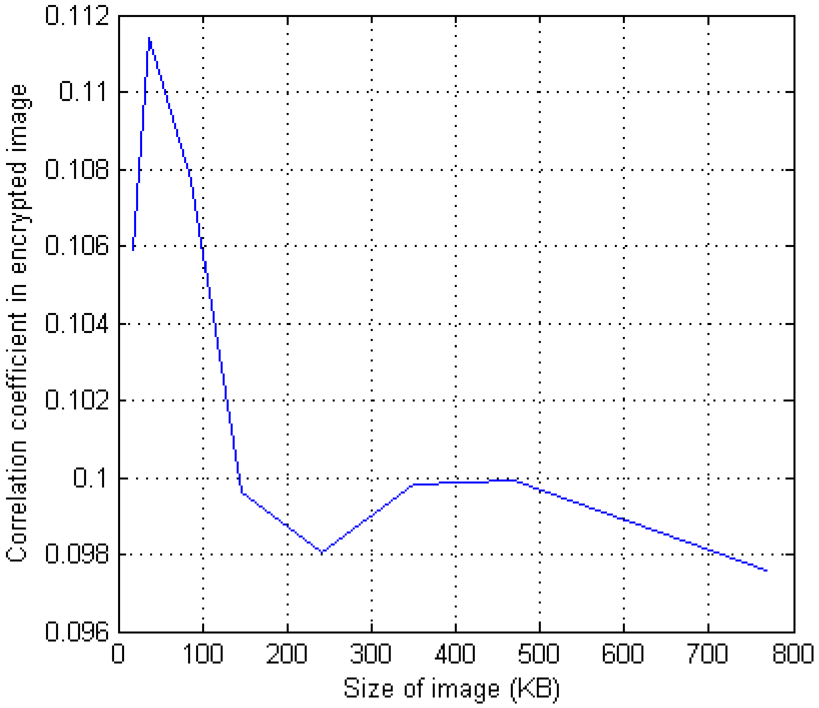

Fig 3: Result of the technique that is based on one-dimensional random scrambling

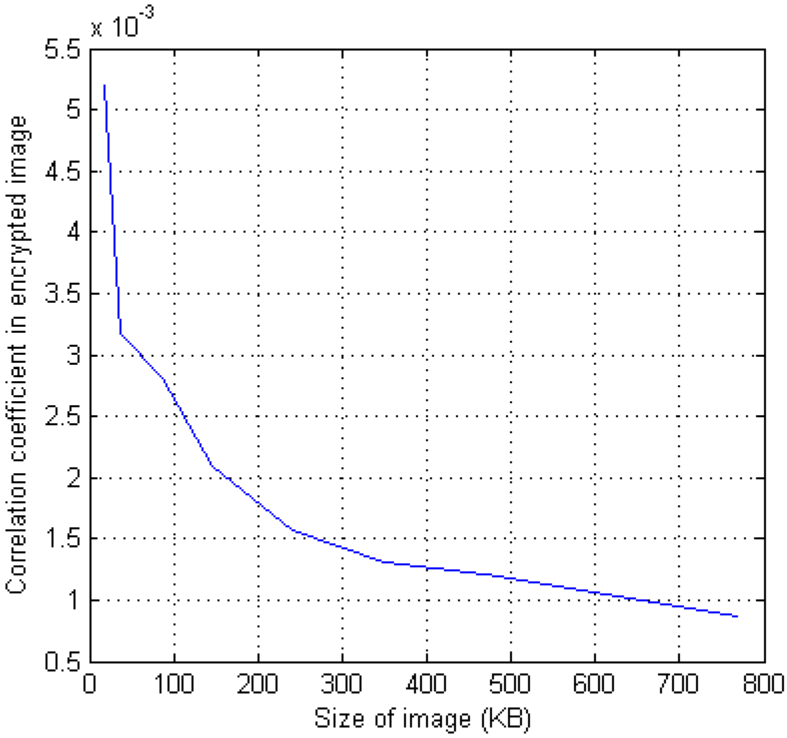

Fig 4: Result of the technique that uses the XOR operation and rotation

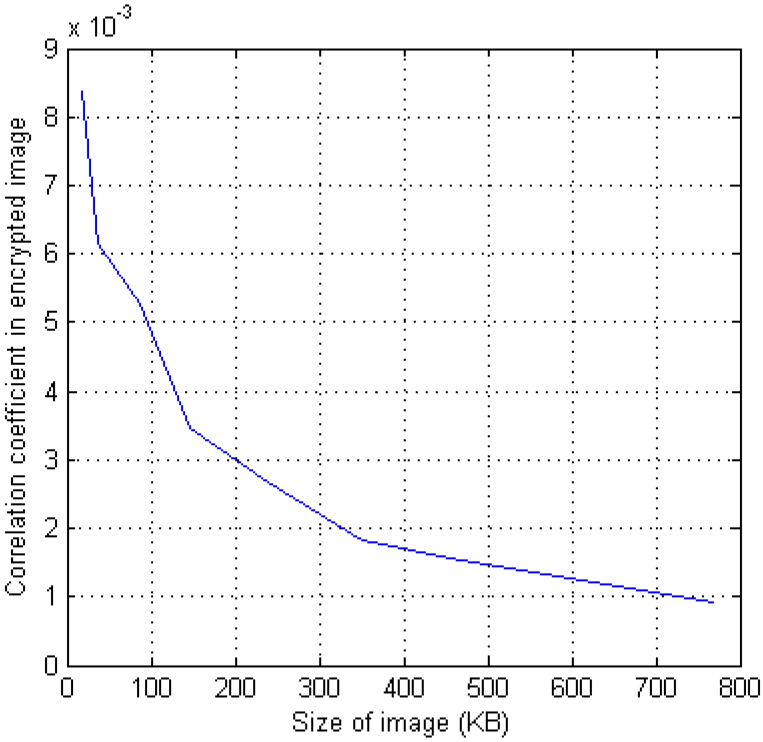

Fig 5: Results of the technique that uses three distinct one-dimensional chaotic maps

4. CONCLUSION

This empirical results disclose that dimension of an image affects the correlation coefficient in the corresponding encrypted image. Moreover, if an image encoding technique utilizes the both scrambling and substitution, then the correlation coefficient is reduced as the size of the image increases. Moreover, correlation coefficient is decreased greatly after each round. However, if an image encryption algorithm applies only shuffling process, then correlation coefficient remains high or gets abatement slowly with respect to the area of the image increases. Reduction in the correlation coefficient in an encrypted image also depends on the cipher approach and number of rounds. However, it is decreased only to some extent. Consequently, an effective design of encoding system is capable to curtail the correlation coefficient to some limit in encoded image gradually after every round.

Thus, this work divulges that an image encryption algorithm should use appropriate procedures to reduce the correlation coefficient in an encoded image. Moreover, the substitution process is extremely essential along with a scrambling method for this purpose.

5. FUTURE WORK

As this experimental work shows that the correlation coefficient is decreased as the size of an image increases. Thus, if users want to send more than one images, they can use an encryption technique that can join all images and then produce single encrypted image. In result, produced encoded image will have decreased correlation coefficient to a great extent and it will create difficulty in statistical analysis of encrypted image.

So there is a need of such technique that can join two or more images and encrypt it. It is also required that in decryption process all joint images should get disjoint without any error.

6. ACKNOWLEDGMENTS

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.

7. 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] 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.

[5] 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.

[6] 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.

[7] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669-1672.

[8] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", International Journal of Security and Its Applications, vol.6, no.1, January 2012, pages: 1-8.

[9] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73 .

[10] D. R.Stinson, Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006.