JOURNAL OF HUMANITARIAN AND APPLIED SCIENCES — مجلة العلوم الإنسانية والتطبيقية
ISSUE 14 – VOLUME 7 — العدد 14 - المجلد 7
ISSN: 2706-9087

Image Encryption Based On Multiplicative Ciphers

Mahmoud H. S. Hasan
Al-asmarya Islamic University College of Information Technology, Zliten – Libya,
tea_mhs@asmarya.edu.ly

تشفير الصور بالاعتماد على التشفير الضربي

محمود حسن سعيد حسن
الجامعة الاسمرية الإسلامية، كلية تقنية المعلومات، زليتن – ليبيا
tea_mhs@asmarya.edu.ly

الملخص

في كل يوم ، تنقتل عبر الشبكات ملايين الصور. البعض يريد نقل بعض الصور بشكل آمن لأن بعضها خاص وسري. يعد التشفير أمرًا ضروريًا لنقل الصور بأمان. يقدم هذا البحث طريقة آمنة لتشفير الصور تعتمد على نظرية المجال المحدود. استخدمنا حقلاً محدودًا يحتوي على 257 عنصرًا. النطاق المقدم هو مجموعة يتم فيها الضرب والجمع والطرح والقسمة، تمامًا كما هو الحال مع أي مجال آخر. تم تنفيذ الخوارزمية باستخدام الضرب والقسمة. استخدمنا حقلاً يحتوي على 257 عنصرًا ، وهو عدد صحيح p عندما يكون p عددًا أوليًا ، والذي يوفر المثال الأكثر شيوعًا للحقول المحدودة. في حالتنا p = 257.نطبقها على الأصفار المضاعفة لتشفير البيانات الثنائية في الصور بايت بايت. تم اختبار النموذج المقترح على صور مختلفة. تم أيضًا قياس إنتروبيا المعلومات ومعامل الارتباط بين وحدات البكسل المجاورة و MSE و PSNR لتقييم مدى تعقيد الصور المشفرة.

الكلمات المفتاحية: cipher, Finite Field, prime numbers, multiplicative ciphers.

ABSTRACT

Every day, the network transfers millions of images. In this paper the attempt has been made to to suggest a method to transfer the photographs securely, because some of them are private and confidential. To transmit images safely, cryptography is essential. This paper provides a secure image encryption method based on finite field theory. We consider a finite field containing 257 elements. A provided domain is a set in which multiplication, addition, subtraction, and division are performed, just like with any other domain. The algorithm was performed using multiplication and division. We consider a finite field containing 257 elements, integer modulo p when p is a prime number, which provides the most common example of finite fields. In our case p = 257. We apply it to multiplicative ciphers to encrypt the binary data in images byte by byte. The proposed model was tested on various images. Information entropy, the correlation coefficient between adjacent pixels, MSE and PSNR were also measured to assess the complexity of encrypted images.

Keywords: cipher, Finite Field, prime numbers, multiplicative ciphers.

1. Introduction

The practice and science of hiding communication from attackers by storing and transmitting it in a format that is unrecognizable to them (Alanazi et al. 152). Many cryptography algorithms depend heavily on finite fields. It can be shown that a finite field's order or the total number of its elements Combined with the arithmetic operations modulo n, the set Z_n of integers $\{0, 1, \dots, n-1\}$ is a commutative ring (Stallings. 109). The method that is widely used to protect data or information. In order to prevent unwanted parties from understanding the message, cryptography encodes it in cipher text form. Encrypting or ciphering is the process of encoding a message. The multiplication cipher will be used to encrypt data in the framework under review in this study. Currently, extensions for multimedia files that are encrypted are taken as pixels in size and a byte, or 8-bit characters. This applies to both text files and graphics. These values and the components of the set Z_{256}. In other words, the ciphering algorithms encode the images and the ciphered texts using the results as modulo 256 values. The message alphabet is then similar to the ring Z_{256}, which unfortunately has a number of zero-divisors, and is equal to a set =$\{0, 1, 2, \dots, 255\}$. It is not recommended to use this ring for cryptography (Ali-Pacha et al. 213). By using 257 instead of 256, we considerably increase the robustness of these cryptosystem methods.

2. Literature Review

The Caesar cipher is a basic substitution cipher with historical significance. Julius Caesar, who employed this code to communicate with his in-group, gave it his name. Every letter in the plaintext of Caesar's messages was shifted three positions to the right in the alphabet to create the message's encryption. Shifted alphabets are the foundation of this cipher (Keshta. 298).

The following function is used to perform the Caesar cipher encryption operation.

$$E(x) = (x + k) \bmod 26 \qquad \dots\dots\dots\dots\dots \quad (1)$$

Where x is the numeric equivalent of a plaintext letter.

The following function is used to perform the Caesar cipher decryption operation.

$$D(c) = (x - k) \bmod 26 \qquad \dots\dots\dots\dots\dots \, (2)$$

Where c is the numeric equivalent of a ciphertext letter.

A Decimation Cipher is similar to a Caesar Cipher but it uses multiplication, rather than addition, by a number key. In order to assure a one-to-one correspondence among the letters of the alphabet, the key number must be relatively prime to 26 (Luciano and Prichett. 2).

The following function is used to perform the Decimation cipher encryption operation.

$$E(x) = (x * k) \bmod 26 \qquad \ldots\ldots\ldots\ldots\ldots (3)$$

Where x is the numeric value of a plaintext letter, and the key number k.

The following function is used to perform the Decimation cipher decryption operation.

$$D(c) = (x * k^{-1}) \bmod 26 \qquad \ldots\ldots\ldots\ldots\ldots (4)$$

Where C is the numeric equivalent of a ciphertext letter. In general, the deciphering key is the multiplicative inverse modulo 26 of the enciphering key k (the inverse must exist since k is relatively prime to 26) (Luciano and Prichett. 2-7).

In (Hana. 213) has proposed a new technique using the affine ciphers with the modulo 257 (as an initial permutation) in any specific algorithm of ciphering to convert a finite set with zero-divisors into a set with no zero-divisors, which is an integral domain. It is clear that employing 257 instead of 256, increased the capacity of the indicator of Euler. The multiplicative Caesar cryptosystem or affine encryption are two examples of cryptosystems that can benefit from this feature.

In (Keshta. 298-307), three programs based on Java, C++, and Python developed to implement the Caesar encryption algorithm are proposed to help information security students and help them understand this basic algorithm. An encrypted message aims to enable the recipient of the message to receive it correctly and prevent snoopers from understanding it. Cryptography is the art and science of converting an original message into a completely unreadable form. The two methods used to convert data into unreadable forms are the transformation method and the substitution method. Caesar cipher uses the substitution method.

3. A Proposed Image Encryption

A Decimation cipher has the following function:

$$E(x) = (x * k) \bmod 256 \qquad \ldots\ldots\ldots\ldots\ldots (5)$$

In addition, the Decimation cipher decryption operation has the following function.

$$D(c) = (x * k^{-1}) \bmod 256 \qquad \ldots\ldots\ldots\ldots\ldots (6)$$

In our case, we use a modified Decimation cipher as follows.

$$\mathrm{E(x)} = \Big(\big((\mathrm{x}+1) * \mathrm{k}\big) \bmod 257\Big) - 1 \qquad \text{……………} (7)$$

Where x is the numeric value of a pixel and the key number k.

In addition, the modified Decimation cipher decryption operation has the following function.

$$\mathrm{D(c)} = \Big(\big((\mathrm{x}+1) * \mathrm{k}^{-1}\big) \bmod 257\Big) - 1 \qquad \text{……………} (8)$$

Where c is the numeric value of a cipher pixel and the key number k.

4. Results AND Discussions

We use several key values to verify the Decimation encryption. We are also focusing on grayscale photos, where each pixel can have a value between 0 and 255.

For this dimension, we selected the "Lena" and "Bird" photos. Fig. 1 and Fig. 2 show that there is more confusion in the plaintext picture when Decimation encryption is used with modulo 257.

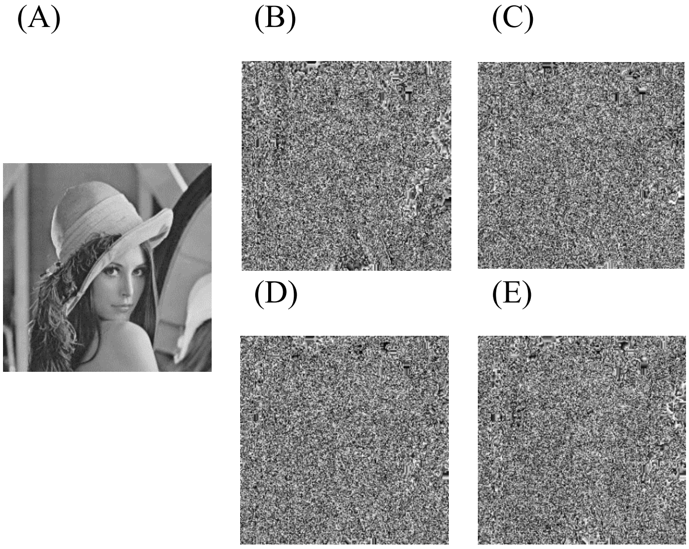

Fig. 1 (A) Original Lena image, (B) Encryption image with key 50, (C) Encryption image with 100, (D) Encryption image with 150, (E) Encryption image with key 200

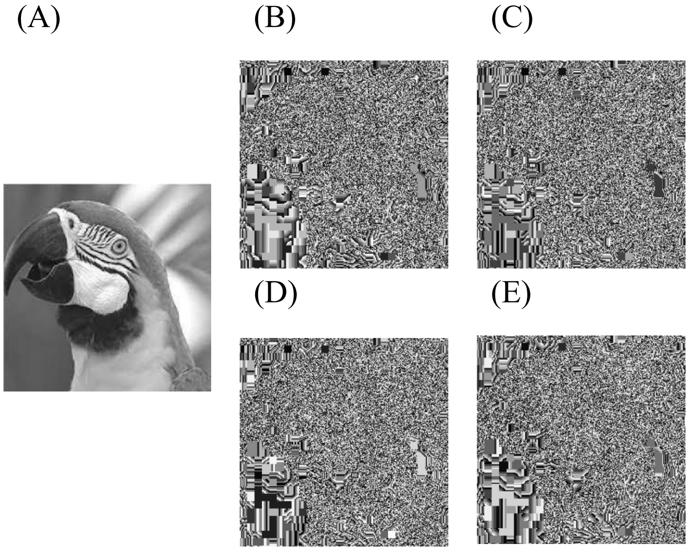

Fig. 2 (A) Original Bird image, (B) Encryption image with key 50, (C) Encryption image with 100, (D) Encryption image with 150, (E) Encryption image with key 200

A. Entropy

Shannon's entropy is a function created by Claude Shannon (Ali-Pacha et al. 216,217). It is a mathematical function that it measures how much information is in a given source of information. Entropy is a measure of the amount of information needed for the receiver to understand what the source has transmitted. Each symbol in a random variable X with n symbols has a probability of P_i appearing, and the entropy H of the source X is given by

$$H(x) = -\sum_{i=1}^{n} P_i \log_2(P_i), P_i = \frac{V_i}{n} \qquad \text{.............. (9)}$$

Where V_i corresponds to the frequency of each number i.

Table 1 and Table 2 display the cipher image’s various entropy values.

Table 1. Entropy for ‘Lena’ image

Encryption key	Plaintext image	Ciphering image
50	7.46203	7.46203
100		7.46203
150		7.46203
200		7.46203

Table 2. Entropy for ‘bird image

Encryption key	Plaintext image	Ciphering image
50	7.63847	7.63785
100		7.63791
150		7.63791
200		7.63791

The entropies of the original image and ciphered images are shown in Table 1 and Table 2. According to the entropy analysis done in Table 1 and Table 2, we can see that the entropy value of the cipher images has the same letter frequencies as the underlying plain images.

B. Histogram analysis

The histogram is calculated using a discrete function that relates the number of pixels that correspond to each intensity value. To calculate the histogram, the number of pixels for each intensity in the image are counted. The histogram can then be viewed as a probability density (Ali-Pacha et al. 218).

Fig. 3 shows the histogram of the plain image and cipher image for the "Lena" image with a variety of keys, and Fig. 4 shows the histogram of the plain image and cipher image for the "Bird" image with a variety of keys. We can observe that whereas the frequency distribution of the pixels in the plain image fluctuates significantly, those in the cipher image histogram are divided equally, which shows that a good encryption image was produced.

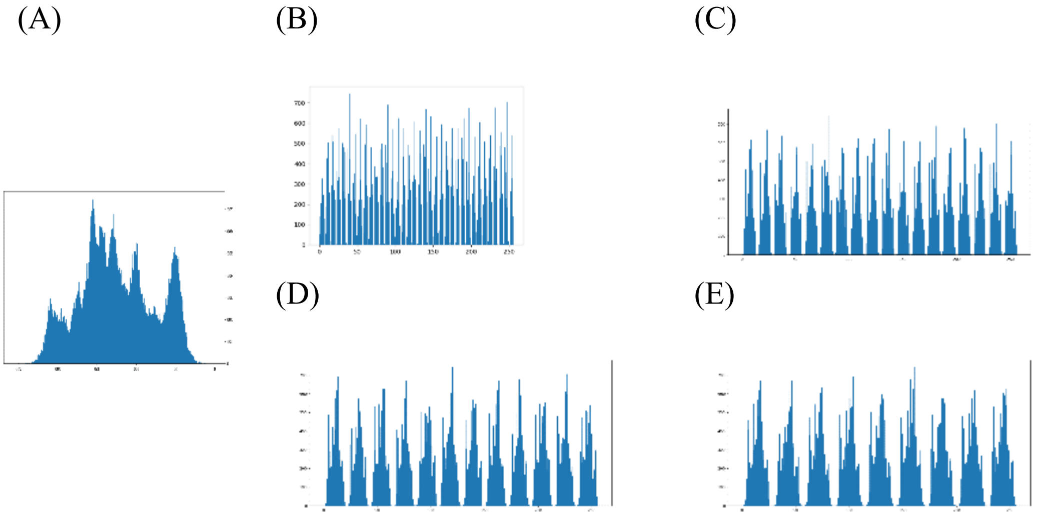

Fig. 3 (A) Histogram of Original Lena image, (B) Histogram encryption image with key 50, (C) Histogram encryption image with 100, (D) Histogram encryption image with 150, (E) Histogram encryption image with key 200

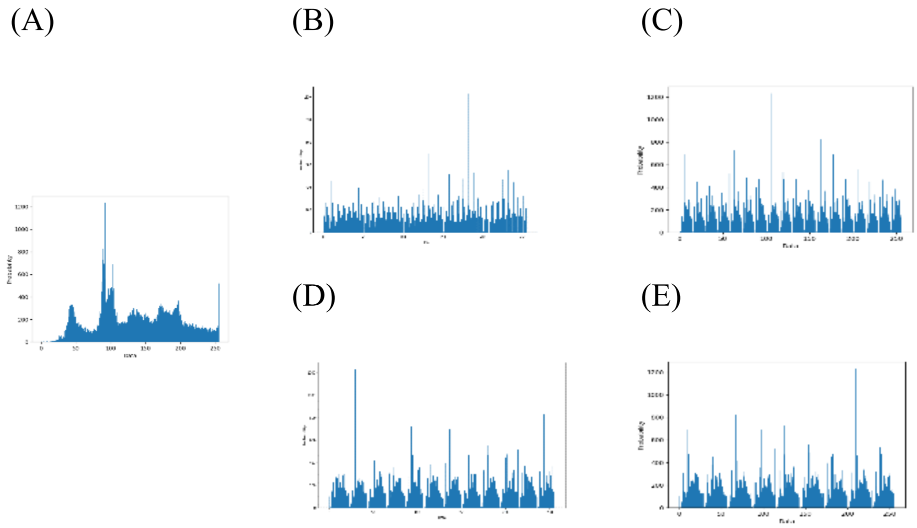

Fig. 4 (A) Histogram of Original Bird image, (B) Histogram encryption image with key 50, (C) Histogram encryption image with 100, (D) Histogram encryption image with 150, (E) Histogram encryption image with key 200

C. Correlation Analysis

The pixel values in typical images that we see on a daily basis are highly correlated with one another. A good cipher image will have very little correlation to the pixel value of its neighboring pixels (L. Singh and K. Singh. 479). The range of the correlation coefficient is between 1 and -1. If the correlation reaches 0, the variables are not correlated (Ali-Pacha et al. 219). This metric can be calculated as in equation (10) (El-Samie et al. 35,36). We can select all pairs of two adjacent pixels from both the plain and encrypted images to measure the correlation coefficient. The relationships between the two diagonal direction pixels in the plain and cipher images are shown in Table 3 and Table 4.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad \ldots\ldots\ldots\ldots\ldots(10)$$

where x and y are the plain- and cipherimages. In numerical computations, the following discrete formulas can be used

$$E(x) = \frac{1}{L}\sum_{l=1}^{l} x_l \qquad \ldots\ldots\ldots\ldots\ldots(11)$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{l}\left(x_l - E(x)\right)^2 \qquad \ldots\ldots\ldots\ldots\ldots(12)$$

$$\mathrm{cov}(x,y) = \frac{1}{L}\sum_{l=1}^{l}\left(x_l - E(x)\right)\left(y_l - E(y)\right) \qquad \ldots\ldots\ldots\ldots\ldots(13)$$

where L is the number of pixels involved in the calculations. The closer the value of r_{xy} to zero, the better the quality of the encryption algorithm will be.

Table 3. The correlation coefficient for the 'LENA' IMAGE

Encryption key	Plaintext image	Ciphering image
50	0.90193	0.03132
100		0.01653
150		0.01214
200		0.02047

Table 4. The correlation coefficient for the 'Bird' IMAGE

Encryption key	Plaintext image	Ciphering image
50	0.93279	0.10077
100		0.05845
150		0.09298
200		0.09817

Table 3 and Table 4 show the correlation between two diagonal adjacent pixels of the clear and ciphering image. It is seen that the neighboring pixels have a strong correlation in the clear 'Lena' image correlation (C= 0.90193), while there is an average correlation (C = 0.02012) in the cipher. Whereas the neighboring pixels in the clear 'Bird' image have a strong correlation (C = 0.93279), while there is an average correlation (C = 0.08759) in the cipher. In the "Lena" and "Bird" images, the poor association between the two neighboring pixels makes it hard to break our cryptography system.

D. MSE AND PSNR Analysis

Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) between the original image and the decrypted image, are both metrics used to evaluate the performance of image encryption algorithms) (El-Samie et al. 38,39). The PSNR which is determined by comparing the original image and the decrypted image was used to assess the decrypted images' quality at the receiver which is defined as follows:

$$\mathrm{PSNR} = 20\,\log_{10}\frac{[255]}{\sqrt{\mathrm{MSE}}} \qquad \ldots\ldots\ldots\ldots\ldots(14)$$

Where MSE is calculated by

$$\mathrm{MSE} = \frac{1}{256\times256}\sum_{i=1}^{256}\sum_{j=1}^{256}\left(A_{ij} - B_{ij}\right)^2 \qquad \ldots\ldots\ldots\ldots\ldots(15)$$

Where the decrypted image's pixel value is $B_{ij}$and the original image's pixel value is A_{ij}.

Table 5 displays the calculated MSE and PSNR of the tested plain images versus the decrypted images (Lena and Bird). Values for MSE are zeros.This demonstrates the effectiveness of the suggested plan.

Table 5. The performance of the proposed Multiplicative Cipher using MSE and PSNR security measures for different gray images with size 256 × 256

Plain Image Name	Measures	Decrypted Image with key 50	Decrypted Image with key 100	Decrypted Image with key 150	Decrypted Image with key 200
Lena	MSE	0	0	0	0
	PSNR	Inf	Inf	Inf	Inf
Bird	MSE	0	0	0	0
	PSNR	Inf	Inf	Inf	Inf

5. Conclusion

This paper attempted to describe a method for encrypting and decrypting images based on a finite field. The goal of this study is to convert a finite set containing zero-divisors into a set with no zero-divisors. The idea, based on this result, is to use the Multiplicative Ciphers with the modulo 257 to extend the number of keys that are used to perform encrypt and decrypt process. This is to increase the security of the specific encryption algorithm. In addition, It is shown that the values of MSE between decrypted image and orginal image are zeros values, which means that the decrypted image is the same as the original image and indicates that the proposed technique is efficient.

References

Ali-Pacha, Hana, et al. “Significant Role of the Specific Prime Number P = 257 in the Improvement of Cryptosystems.” Notes on Number Theory and Discrete Mathematics, vol. 26, no. 4, Nov. 2020, pp. 213–222, 10.7546/nntdm.2020.26.4.213-222. Accessed 9 Nov. 2022.

Alanazi Hamdan., Zaidan B. and Zaidan A., New Comparative Study between DES, 3DES and AES within Nine Factors, Journal Of Computing. Vol. 2 , Issue 3, 2010, Pp.152-157.

Babu Sriramoju, "Modification Affine Ciphers Algorithm For Cryptography Password", International Journal of Research In Science & Engineering, Volume: 3, no: 2, March-April 2017, pp. 346-351.

Chen, Guanrong, et al. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps." Chaos, Solitons & Fractals, vol. 21, no. 3, July 2004, pp. 749–761, www.sciencedirect.com/science/article/pii/S0960077903006672, 10.1016/j.chaos.2003.12.022. Accessed 16 Aug. 2019.

Dawahdeh, Ziad E., et al. "A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher." Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, July 2018, pp. 349–355, 10.1016/j.jksuci.2017.06.004.

Fathi E Abd El-Samie. Image Encryption : A Communication Perspective. Boca Raton Florida, Crc Press, Tayllor & Francis Group, 2014.

Keshta Ismail, "Caesar Cipher Method Design and Implementation", International Journal of Computer Science and Information Security, Vol. 16, No. 4, April 2018, pp. 298-307

Luciano, Dennis, and Gordon Prichett. "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems." The College Mathematics Journal, vol. 18, no. 1, Jan. 1987, p. 2, 10.2307/2686311.

L. Singh and K. Singh, "Image Encryption Using Elliptic Curve Cryptography." Procedia Computer Science, vol. 54, 2015, pp. 472–481, 10.1016/j.procs.2015.06.054. Accessed 2 Mar. 2020.

Stallings, William. Cryptography and Network Security : Principles and Practice : William Stallings. Upper Saddle River, N.J., Pearson/Prentice Hall, 2006.

Yan, Song Y. Computational Number Theory and Modern Cryptography. Hoboken, John Wiley & Sons, Inc, 2013.