第 48 卷 第 12 期
2021 年 12 月

湖南大学学报（自然科学版）
Journal of Hunan University (Natural Sciences)

Vol. 48 No. 12
December 2021

Open Access Article

A Simple, Efficient, Secure and Accurate Method of Speech Signal Cryptography

Rashad J. Rasras[1], Mutaz Rasmi Abu Sara[2], Ziad Alqadi[1]

[1] Department of Computer Engineering, Al-Balqa' Applied University, Amman, Jordan

[2] IT Department, Palestine Ahliya University, Bethlehem, Palestine

Abstract: Protecting data, including digital speech signals, is an important and vital task. The problem of all methods used in data encryption lies in the difficulty of generating the secret private key used in the encryption process. In some cases, the process of penetrating the key is available or easy. This research aims to develop a new, simple, highly secure, and efficient encryption-decryption method. The developed new method uses a digital color image as an image key; this key will be used to generate the private key. A huge image key is used to extract the necessary private key used in the cryptography process. The introduced method is tested and implemented to prove the efficiency issues and maintain high values for the quality parameters during the encryption and decryption processes.

Keywords: speech, image key, cryptography, mean square error, throughput.

一种简单、高效、安全、准确的语音信号加密方法

摘要：保护包括数字语音信号在内的数据是一项重要且至关重要的任务。 数据加密中使用的所有方法的问题在于难以生成加密过程中使用的秘密私钥。 在某些情况下，穿透钥匙的过程是可行的或容易的。 本研究旨在开发一种新的、简单的、高度安全的、高效的加解密方法。 开发的新方法使用数字彩色图像作为图像键； 该密钥将用于生成私钥。 巨大的图像密钥用于提取加密过程中使用的必要私钥。 引入的方法经过测试和实施，以证明效率问题并在加密和解密过程中保持质量参数的高值.

关键词：语音、图像密钥、密码学、均方误差、吞吐量.

1. Introduction

Digital images [1], [2] are available everywhere. They can be obtained easily and at no cost and can be generated easily due to the multiplicity of means and tools available for this purpose [3], [4]. The digital image consists of three channels, as shown in Figure 1. The first channel is assigned to the red color, the second to the green color, and the third channel to the blue color. Each channel is represented by a two-dimensional matrix containing the values between.

The digital image represents a huge data collection that can be used for many vital applications, the most important of which is the data encryption process [5]-[7].

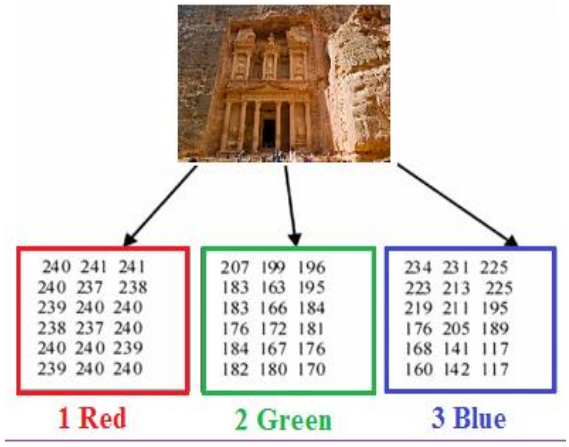


Fig. 1 Digital color image matrices

Received: August 11, 2021 / Revised: October 9, 2021 / Accepted: November 5, 2021 / Published: December 30, 2021

About the authors: Rashad J. Rasras, Department of Computer Engineering, Al-Balqa' Applied University, Amman, Jordan; Mutaz Rasmi Abu Sara, IT Department, Palestine Ahliya University, Bethlehem, Palestine; Ziad Alqadi, Department of Computer Engineering, Al-Balqa' Applied University, Amman, Jordan

The elements of an image matrix are integer values between 0 and 255, but sometimes, in order to implement something, we may need other fractional values between zero and one; here, we can convert the RGB color image to NTSC (YIQ) image applying equation (1):

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

Below is how to perform the conversion:

$$Y = 0.299\,R + 0.587\,G + 0.114\,B$$
$$I = 0.596\,R - 0.275\,G - 0.321\,B$$
$$Q = 0.212\,R - 0.523\,G + 0.311\,B$$

Figure 2 shows an image example, while figure 3 shows the YIQ image obtained from the RGB color image.

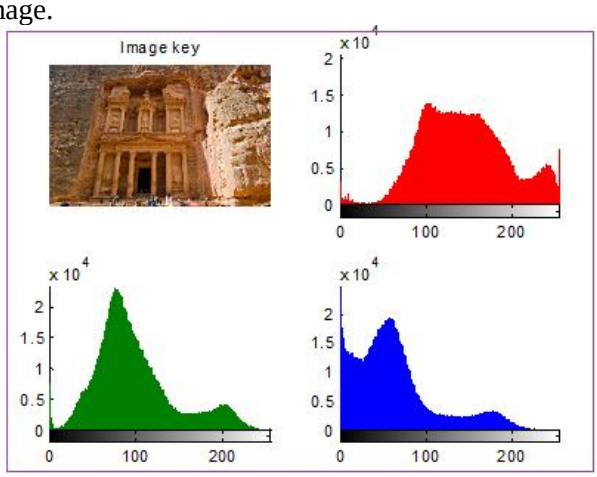


Fig. 2 RGB color image example

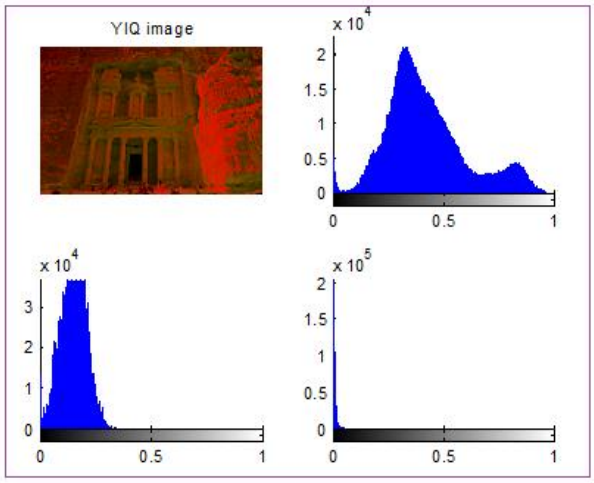


Fig. 3 YIQ equivalent

A speech signal [8] [9]is a wave that spreads in many mediums such as solid, liquid, and gaseous media, as it is used as a means of communication between living organisms. The speech is an analog signal [11], [12], which can be converted to a digital signal using analog to digital converter (ADC), which performs sampling, quantization, and encoding as shown in Figures 4 and 5:

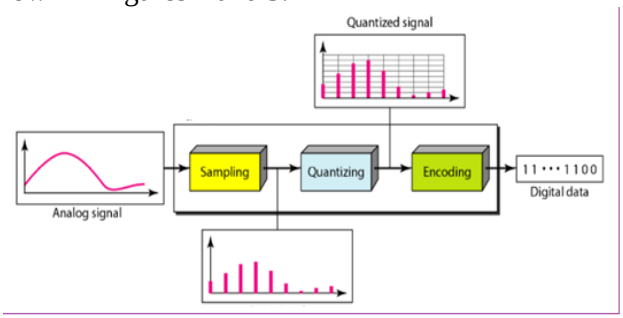


Fig. 4 ADC functions

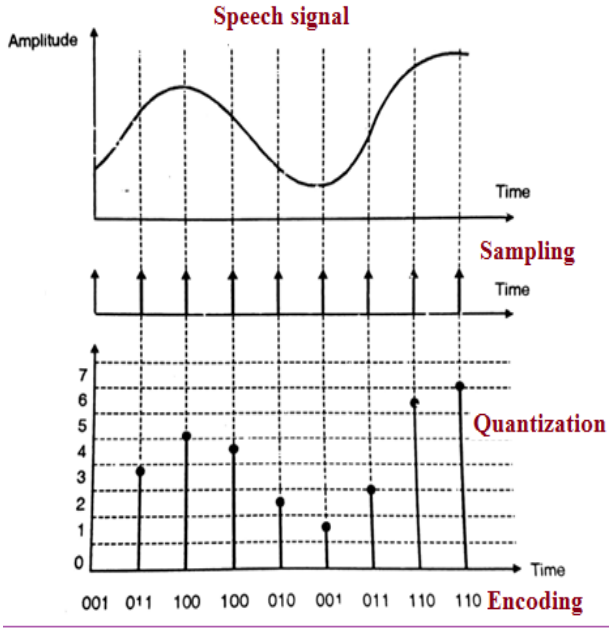


Fig. 5 Operation to Covert Analogue Speech to Digital Speech

The digital speech signal is represented by one (mono speech) or two (stereo speech) column matrices. Each element (sample) in this matrix represents the speech amplitude at a time, and the number of the sample (speech size) will depend on the sampling frequency and the recording time [10].

Sometimes, the speech signal can be considered confidential, and we can apply speech encryption-decryption to protect it.

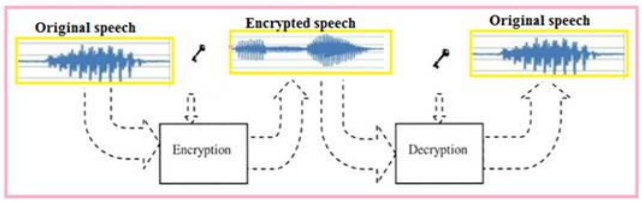


Fig. 6 Speech cryptography

Speech cryptography can be done, as shown in Figure 6, using a method of cryptography and a secret private key (PK) to protect the encrypted speech from being hacked by any third party who is not authorized to listen or use the speech file.

The encryption phase must fully destroy the original speech by maximizing mean square error (MSE) [13], [14] between the original and encrypted speeches (or

minimize the peak signal to noise ratio (PSNR) between them), while the decryption phase must maximize PSNR and minimize MSE between the original and the decrypted signals.

MSE and PSNR [15] can be calculated using equations 1 and 2.

MSE between messages S and R, n: message length

$$MSE_{SR} = \frac{1}{N}\sum_{j=0}^{n-1}[S(j) - R(j)]^2, N = n \quad (1)$$

$$PSNR_{SR} = 10 * \log_{10}\frac{(MAX_i)^2}{MSE_{SR}} \quad (2)$$

Any method of cryptography can be considered good if it satisfies the following:

- Provides good values for quality parameters (MSE and PSNR), as shown in Table 1.

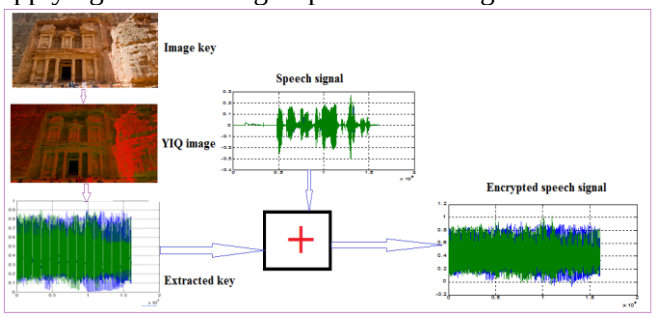
Table 1 Quality parameters

Between the speech files	MSE	PSNR
Original and encrypted	Very high	Very low
Original and encrypted	Very high	Very low

- Secure; by making the hacking process impossible, security can be achieved using PK.
- Efficient by maximizing the method throughput.
- Simple to use and implement.

2. The Proposed Method

The proposed method uses a digital color image as a private key. This image is kept with the sender and receiver, and any other person knows it. In this way, we can ensure the security of the proposed method by protecting the encrypted signal from hacking. The process of encrypting speech signal can be performed applying the following steps shown in Figure 7:



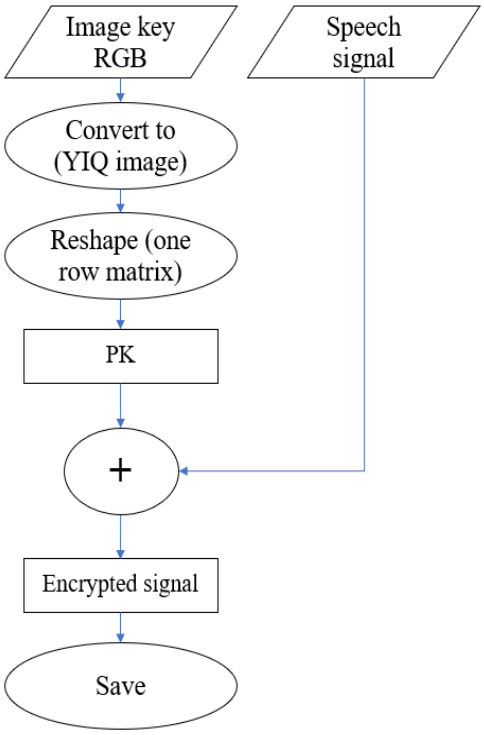
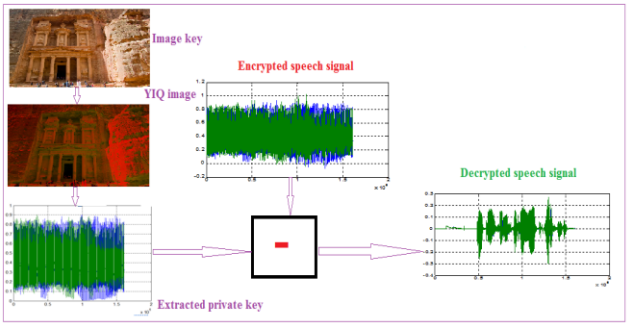


Fig. 7 Proposed encryption process

Step 1: Select the image key.
Step 2: Convert the RGB image to the YIQ image.
Step 3: Reshape the image into a one-row matrix.
Step 4: Get the speech signal.
Step 5: Reshape the signal to the one-row matrix.
Step 6: Extract an array with equal signal length from the row image; this array is used as a PK.
Step 7: Add PK to the speech signal to get the encrypted signal.
Step 8: Reshape back the encrypted signal.
Step 9: Save the encrypted speech signal.

The decryption phase, as shown in Figure 8, can be performed applying the following steps:



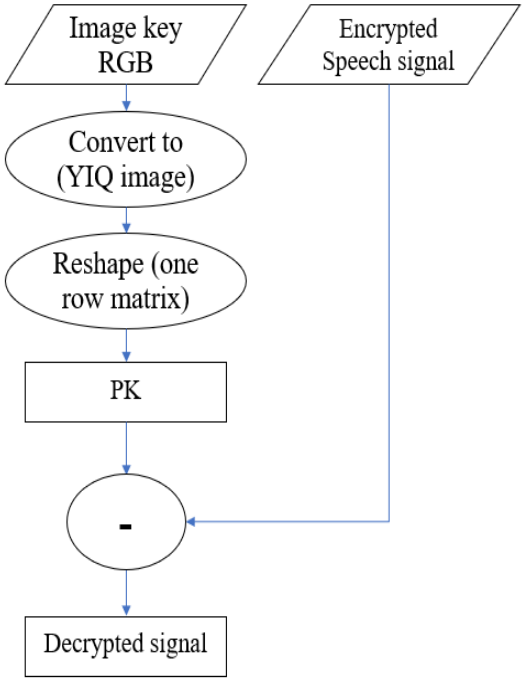


Fig. 8 Proposed decryption process

Step 1: Get the image key.
Step 2: Convert the RGB image to the YIQ image.
Step 3: Reshape the image into the one-row matrix.
Step 4: Get the encrypted speech signal.
Step 5: Reshape the signal to the one-row matrix.
Step 6: from the row image, extract an array with equal signal length; this array is used as a PK.
Step 7: Subtract PK from the speech signal to get the decrypted signal.
Step 8: Reshape back the encrypted signal.

3. Implementation and Experimental Results

The software program was developed using MATLAB as described below to study the practical results of encryption and decryption algorithms.

```
close all,clear all,clc
%Encryption
a=imread('E:\my_images\a4.jpg');% image key
b=rgb2ntsc(a); [n1 n2 n3]=size(b);b1=reshape(b,1,n1*n2*n3);
[v1 fs]=wavread('a1.wav');[n4 n5]=size(v1);
sound(v1,fs)
tic
v2=reshape(v1,1,n4*n5);
vkey=b1(1,1:n4*n5);
ff=reshape(vkey,n4,n5);
ev=v2+vkey;
ev=reshape(ev,n4,n5);
toc
sound(ev,fs)
dddd=input('press any key');
wavwrite(ev,fs,'a1en.wav');
```

```
%Decryption
a=imread('E:\my_images\a4.jpg');%the same image key
imshow(a)
b=rgb2ntsc(a);
[n1 n2 n3]=size(b);
b1=reshape(b,1,n1*n2*n3);
[ev fs]=wavread('a1en.wav');
ev1=reshape(ev,1,n4*n5);
vkey=b1(1,1:n4*n5);
dv=ev1-vkey;
dv1=reshape(dv,n4,n5);
sound(dv1,fs)
```

The program was implemented using various images and speeches; Figure 9 shows an example output of the implementation, while Figure 10 shows the used images in the implementation.

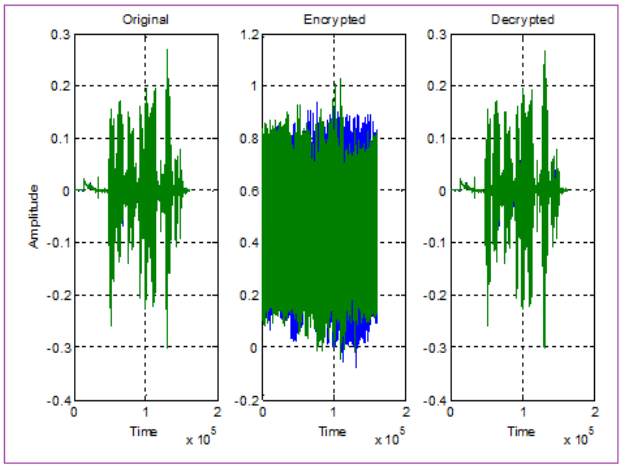


Fig. 9 Output example

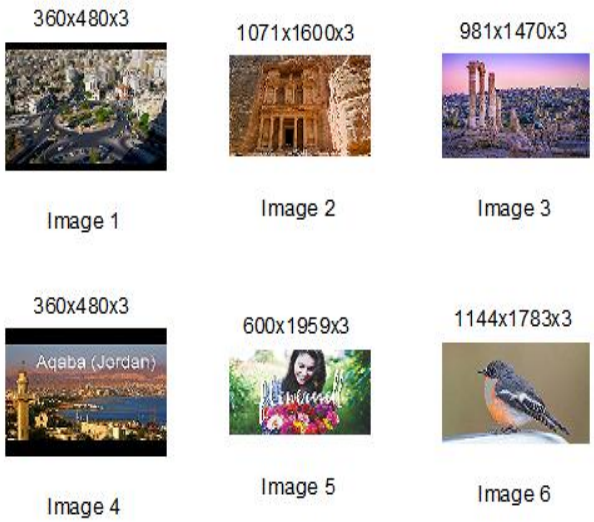


Fig. 10 Used images

Image 2 was selected as a private key, this image was used to encrypt-decrypt various speech signals, and Table 2 shows the obtained experimental results:

Now we fix the image key (image 2) in the encryption phase and use another image in the decryption phase. Table 3 shows the obtained results for encryption-decryption speech 1:

From the obtained results shown in the above tables, we can see the following:

- The proposed method is very secure, and it is very difficult to hack a huge image key.

- The method is very accurate by providing good quality parameters when encrypting speech signals and decrypting the signal.
- The proposed method is efficient by providing a high throughput (on average 5.6003e+007 samples per second).
- Using different image keys in the decryption process will totally destroy the signal.
- The method is very simple to be implemented.

Table 2 Results of using Image 2 as an image key

Speech signal number	Size(samples)	Between original and encrypted speeches	Between original and decrypted speeches	Encryption/decryption time(second)	Speech signal number	Size(samples)
		MSE	PSNR	MSE (close to zero)	PSNR	
1	321536	0.1302	20.9460	2.2934e-035	771.2833	0.006000
2	200704	0.1293	19.7702	1.5143e-035	773.2095	0.004000
3	227328	0.1294	19.4915	1.4544e-035	773.7475	0.004000
4	430080	0.1324	20.0819	2.3328e-035	772.4317	0.006000
5	172032	0.1291	18.6430	8.5288e-036	758.2780	0.003000
6	133120	0.1296	18.4346	8.6144e-036	752.1292	0.003000
7	212992	0.1294	18.4067	1.0444e-035	765.6733	0.004000
8	272384	0.1296	19.3296	1.0010e-035	770.7074	0.004000
9	17472	0.1319	19.2016	3.6398e-035	768.1422	0.001000
10	28473	0.1308	29.2609	3.4685e-034	770.4410	0.001000
1	321536	0.1302	20.9460	2.2934e-035	771.2833	0.006000
2	200704	0.1293	19.7702	1.5143e-035	773.2095	0.004000
3	227328	0.1294	19.4915	1.4544e-035	773.7475	0.004000
Average	2.0161e+005					0.0036
Throughput		2.0161e+005/0.0036=5.6003e+007 samples per second				

Table 3 Encryption-decryption using different image keys (one for encryption and other for decryption)

Image number used as an image key in the decryption phase	Between original and encrypted speeches		Between original and decrypted speeches	
	MSE	PSNR	MSE	PSNR
1	0.1302	20.9460	0.0946	23.3445 (Fully destroyed)
2 (the same image)	0.1302	20.9460	2.2934e-035	771.2833
3	0.1302	20.9460	0.0672	25.0347 (Fully destroyed)
4	0.1302	20.9460	0.0914	23.7425 (Fully destroyed)
5	0.1302	20.9460	0.1707	12.5579 (Fully destroyed)

4. Conclusion

A new method of speech signal encryption-decryption was introduced. The method uses a digital color image as an image key; that will be used to generate the private key. Using image keys increases the level of security and thus highly protects the speech signal from being hacked. The proposed method gave good values for MSE and PSNR in both phases: encryption and decryption. The obtained experimental result showed that the method is very efficient by maximizing the method throughput by minimizing the encryption-decryption time.

References

[1] BARAKAT M T, ZAINI H G, & ALQADI Z. Text File Encryption_Decryption Using Key Quotient and Remainder. *International Journal of Engineering Technology Research & Management*, 2021, 5(4): 9-21.

[2] ALQADI Z, & HUSSEIN M E. Window Averaging Method to Create a Feature Victor for RGB Color Image. *International Journal of Computer Science and Mobile Computing*, 2017, 6(2), 60-61.

[3] ZAHRAN B, AYYOUB B, NADER J, & ALQADI Z. Suggested Method to Create Color Image Features Victor. *Journal of Engineering and Applied Sciences*, 2019, 14(7): 2203-2207.

[4] AL-DWAIRI M O, ALQADI Z, ABUJAZAR A A, & ZNEIT R A. Optimized True-Color Image Processing. *World Applied Sciences Journal*, 2010, 10(8): 1175-1182.

[5] MOUSTAFA A A, & ALQADI Z, Color Image Reconstruction Using a New R'G'I Model. *Journal of Computer Science*, 2009, 5(4): 250-254.

[6] AL AZZEH J, ALHATAMLEH H, ALQADI Z, & KHALIL M. Creating a Color Map to be used to Convert a Gray Image to Color Image. *International Journal of Computer Applications*, 2016, 153(2): 31-34.

[7] ABU-EIN A, ALQADI Z, & NADER J. A Technique of Hiding Secrets Text in Wave File. *International Journal of Computer Applications*, 2016, 9(2): 96-103.

[8] AL-DWAIRI M O, HENDI A Y, SOLIMAN M S, & ALQADI Z. A new method for voice signal features creation, *International Journal of Electrical and Computer Engineering*, 2019, 9(5): 4092-4098.

[9] AL-RAWASHDEH A, & ALQADI Z. Using wave equation to extract digital signal features. E*ngineering, Technology & Applied Science Research*, 2018, 8(4): 1356-1359.

[10] NADIR J, ABU-EIN A, & ALQADI Z. A Technique to Encrypt-decrypt Stereo Wave File. *International Journal of Computer and Information Technology*, 2016, 5(5): 465-470.

[11] ALQADI Z., HINDI A Y, & MAJED O D. Procedures for Speech Recognition Using LPC and ANN. *International Journal of Engineering Technology Research & Management*, 2020, 4(2): 48-55.

[12] HINDI A Y, AL-DWAIRI M O, & ALQADI Z. Analysis of Digital Signals using Wavelet Packet Tree. *International Journal of Computer Science and Mobile Computing*, 2020, 9(2): 96-103.
[13] AL-DWAIRI M O, HENDI A, & ALQADI Z. An efficient and highly secure technique to encrypt-decrypt color images. *Engineering, Technology & Applied Science Research*, 2019, 9(3): 4165-4168.
[14] BILAL Z, ALQADI Z, & NADER J. A Comparison Between Parallel and Segmentation Methods Used for Image Encryption-Decryption. *International Journal of Computer Science & Information Technology*, 2019, 8: 127-133.
[15] ALQADI Z, KHRISAT M S, & HINDI A. Digital color image encryption-decryption using segmentation and reordering. *International Journal of Latest Research in Engineering and Technology*, 2020, 6(5): 6-12.

参考文:

[1] BARAKAT M T、ZAINI H G, 和 ALQADI Z。使用密钥商和余数的文本文件加密_解密。国际工程技术研究与管理杂志, 2021, 5(4): 9-21.

[2] ALQADI Z 和 HUSSEIN M E. 为 RGB 彩色图像创建特征胜利者的窗口平均方法。国际计算机科学与移动计算杂志, 2017, 6(2), 60-61.

[3] ZAHRAN B、AYYOUB B、NADER J 和 ALQADI Z. 创建彩色图像特征胜利者的建议方法。工程与应用科学学报, 2019, 14(7): 2203-2207.

[4] AL-DWAIRI M O、ALQADI Z、ABUJAZAR A A 和 ZNEIT R A。 优化的真彩色图像处理。世界应用科学杂志, 2010, 10(8): 1175-1182。

[5] MOUSTAFA A A 和 ALQADI Z, 使用新的 R'G'I 模型进行彩色图像重建。计算机科学杂志, 2009, 5(4): 250-254.

[6] AL AZZEH J、ALHATAMLEH H、ALQADI Z 和 KHALIL M. 创建用于将灰色图像转换为彩色图像的颜色图。国际计算机应用杂志，2016，153（2）：31-34。

[7] ABU-EIN A、ALQADI Z 和 NADER J. 在 Wave 文件中隐藏秘密文本的技术。国际计算机应用杂志, 2016, 9(2): 96-103.

[8] AL-DWAIRI M O, HENDI A Y, SOLIMAN M S, 和 ALQADI Z. 一种新的语音信号特征创建方法, 国际电气与计算机工程杂志, 2019, 9(5): 4092-4098.

[9] AL-RAWASHDEH A, 和 ALQADI Z. 使用波动方程提取数字信号特征。工程、技术与应用科学研究, 2018, 8(4): 1356-1359.

[10] NADIR J、ABU-EIN A 和 ALQADI Z。一种加密-解密立体波文件的技术。国际计算机与信息技术杂志, 2016, 5(5): 465-470.

[11] ALQADI Z.、HINDI A Y 和 MAJED O D. 使用 LPC 和 ANN 进行语音识别的程序。国际工程技术研究与管理杂志, 2020, 4(2): 48-55.

[12] HINDI A Y、AL-DWAIRI M O 和 ALQADI Z. 使用小波包树分析数字信号。国际计算机科学与移动计算杂志, 2020, 9(2): 96-103.

[13] AL-DWAIRI M O、HENDI A 和 ALQADI Z。一种高效且高度安全的彩色图像加密和解密技术。工程、技术与应用科学研究, 2019, 9(3): 4165-4168.

[14] BILAL Z、ALQADI Z 和 NADER J。用于图像加密-解密的并行和分割方法的比较。国际计算机科学与信息技术杂志，2019，8：127-133。

[15] ALQADI Z、KHRISAT M S 和 HINDI A. 使用分割和重新排序的数字彩色图像加密解密。国际工程与技术最新研究杂志，2020, 6(5)：6-12。