IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 1, February, 2022, pp. 173-178
Journal homepage: http://iieta.org/journals/ts

Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography

Mua'ad M. Abu-Faraj[1*], Khaled Aldebei[2], Ziad A. Alqadi[3]

[1] Department of Computer Information Technology, The University of Jordan, Aqaba 77110, Jordan
[2] Department of Information Technology, The University of Jordan, Aqaba 77110, Jordan
[3] Electrical Engineering Department, Albalqa Applied University, Amman 15008, Jordan

Corresponding Author Email: m.abufaraj@ju.edu.jo

https://doi.org/10.18280/ts.390117

Received: 7 November 2021
Accepted: 3 January 2022

Keywords:
cryptography, throughput, speed up, data quality, MSE, PSNR

ABSTRACT

Some digital data circulated through various social media, regardless of its nature, requires high-level protection and security for various reasons. In this research, a multi-purpose method will be presented to be used in encrypting SMS messages, text files regardless of their size, digital images of all kinds and sizes, and audio files of all kinds and sizes. The proposed method will be examined to prove its efficiency, and the practical results will be compared with the implementation results of other internationally approved methods to show the extent to which the method improves efficiency indicators. It will be shown how to use digital color image to generate a highly secure private key which will make the process of hacking impossible. The Quality of the encrypted and decrypted images will be examined to justify the use of the proposed method.

1. INTRODUCTION

In recent times, the process of circulating digital data through various social media has increased, and a lot of this data, whether it is short text messages or text files of varying size, or digital images of various types (color, gray and binary) and multiple sizes, or audio files of various types (mono and stereo) and various sizes require protection and to a high degree because Enable intruders to penetrate it or enable unauthorized parties to understand the content of this data for the following reasons [1-5]:

- Digital data may be confidential or of a private nature, and any unauthorized person or entity must be prevented from accessing and understanding it.
- Digital data, especially digital images, may contain confidential or private data.

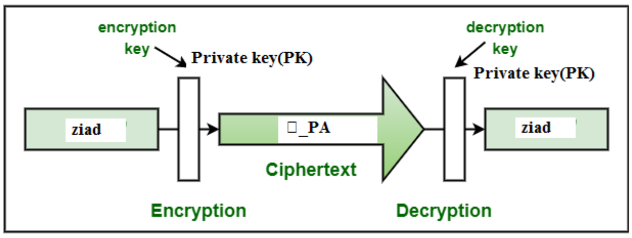


Figure 1. Data cryptography

One of the popular methods used to protect data is data cryptography, which means encryption and decryption. Encryption process is used to destroy the data so as to become un understandable, while decryption process is used to recover the original data from the encrypted one as shown in Figure 1.

Data cryptography usually applied by using a private (secret) key which is known by the sender and receiver, this key can be used in implementing a set of logical and arithmetic operation to generate the encrypted and decrypted data.

The quality of the encrypted and decrypted data can be measured by mean square error (MSE) and/or peak signal to noise ratio (PSNR). The value of MSE must be very high and the PSNR value must be very low using the encrypted data (this means fully destruction of the original data), while MSE must be closed to zero and PSNR must be closed to infinite (or very high) for the decrypted data (this means fully data recovery), MSE and PSNR can be calculated using Eqns. (1) and (2).

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

$$PSNR_{\mathrm{sk}} = 10*\log_{10}\frac{\left(MAX_{\mathrm{j}}\right)^2}{MSE_{\mathrm{sR}}} \tag{2}$$

Any method of encryption and decryption is considered a good method if it achieves the following:

- The private key must be secure and difficult to penetrate; this will increase the protection degree.
- It must be efficient by maximizing the method throughput (number of bytes encrypted/decrypted in a second).
- The method must give the necessary value of MSE and PSNR after executing the encryption and decryption phases.
- The method must be simple and easy to implement.
- The method must be easily used to encrypt/decrypt any type of data (texts, images, speeches).

Color digital images are now available everywhere and can be obtained easily and at no cost. The color image is a huge data store that can easily be employed to generate a private secret key if the specified image is kept secret between the sender and receiver.

The digital image is processed in easy ways and it can be converted into a special type that fits with the audio files or changed its size to match the size of the data to be encrypted or decrypted.

2. RELATED WORKS

Many methods were introduced for data cryptography, here we will focus on the symmetric method, the most popular of them are: DES [6-9], 3DES [9-12], AES [12-18], RC2 [19], RC6 [20] and Blowfish [21, 22]. Table 1 shows the main features of these methods. These methods were used to encrypt-decrypt messages and text file and the following weaknesses:

- The encryption-decryption throughput rapidly decreased when the input data size increases.
- The private keys are short and can be hacked, this will decrease the level of security.
- Input data must be divided into blocks, each block must be separately encrypted-decrypted and here an extra time will be needed for data dividing and assembling.
- Extra time is needed for key generation required for various rounds.
- A set of complex logical and arithmetic operations is required.
- These methods are designed to encrypt-decrypt messages and text file and the efficiency of using them to encrypt-decrypt digital images will be very low because of the images sizes.
- It is not easy to use these methods to encrypt-decrypt digital speech files. Speech file is constructed from samples; each sample is represented by a double type data. The introduced methods were design to treat integer value.

Table 1. Introduced methods of data cryptography features

Feature	DES	3DES	AES	RC2	RC6	Blowfish	Proposed
Data block size	64 bits	64	128	64 bits	128 bits	64 bits	Any size, Text size
PK length	56 bits	Three 56-bit	128, 192, or 256	1-128 bits	128-2040 bits	32-448 bits	Size of selected block or text file size
Principle	Feistel Cipher [1]	Feistel Cipher	Feistel Cipher	Block cipher	Block cipher [10]	Feistel Cipher	Image selecting, resizing
Rounds	14	48	16	18	20	16	No rounds
Operation	Expansion Permutation, Xor, S-box, P-box, Xor and Swap [2-5]	Expansion Permutation, Xor, S-box, P-box, Xor and Swap	Sub bytes, Shift rows, Mix columns, Add round [10-13] keys	Sub bytes, Shift rows, Mix columns, Add round keys	Sub bytes, Shift rows, Mix columns, Add round keys	substitution and permutation [1-5]	resizing, XORing
Security	Low	Low	High	High	High	High	Very high
Speed	slow	Slow	slow	slow	slow	slow	Very fast
Image encryption	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Very easy
Speech encryption	Difficult	Difficult	Difficult	Difficult	Difficult	Difficult	Easy
Simplicity	Not simple	Not simple	Not simple	Not simple	Not simple	Not simple	Very simple

3. THE PROPOSED METHOD

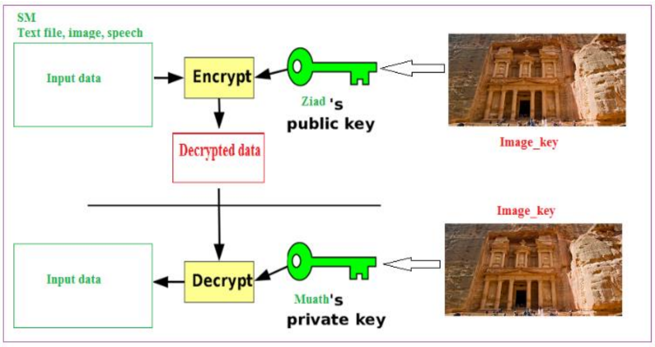


Figure 2. Proposed method of data cryptography

The proposed method uses a digital color image as an image-key (see Figure 2); this image must be kept in secret. The image-key must be agreed upon by the sender and the receiver, so that it will be saved without the process of sending it, and it can be replaced easily by another image any time and when needed without modifying the method of data cryptography.

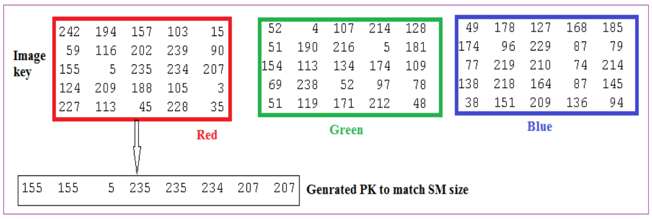
One of the most important advantages of using a digital color image as a key image lies in the following:

- Ease of obtaining the digital image at no cost.
- Multiple digital image acquisition sources.
- Ease of digital image processing.
- Possibility to resize the image to obtain vectors with a specified length.
- The possibility of converting the values in the digital image from range 0 to 255 to range -1 to 1 to suit the data to be processed.

The proposed method can be used to encrypt-decrypt any kind of data (short message (SM), text file, digital image, and speech file), there is no limitation on the input data size, here the data size can be varied and the image-key can be resized to match the input data size. The image-key pixel value falls in the range 0 to 255, so it is necessary to convert the image-key to NTSC image with pixel value range from -1 to 1, the NTSC image value here will be closed to the speech file values, this can be done applying Eq. (3).

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (3)$$

Any color image can be resized to get an array with a specified length. This can be done by applying image resizing. Figures 3, 4 and 5 illustrate an example of image-key resizing and converting to NTSC image applying Eq. (3).



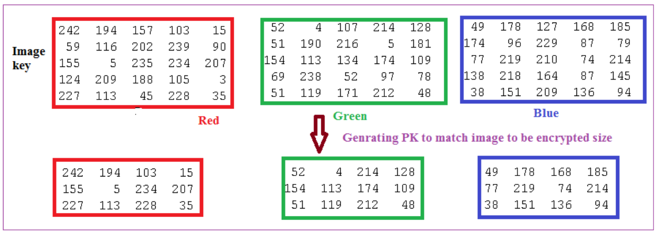
242	194	157	103	15
59	116	202	239	90
155	5	235	234	207
124	209	188	105	3
227	113	45	228	35

52	4	107	214	128
51	190	216	5	181
154	113	134	174	109
69	238	52	97	78
51	119	171	212	48

49	178	127	168	185
174	96	229	87	79
77	219	210	74	214
138	218	164	87	145
38	151	209	136	94

155	155	5	235	235	234	207	207

Figure 3. Private key generation for message encryption



242	194	157	103	15
59	116	202	239	90
155	5	235	234	207
124	209	188	105	3
227	113	45	228	35

52	4	107	214	128
51	190	216	5	181
154	113	134	174	109
69	238	52	97	78
51	119	171	212	48

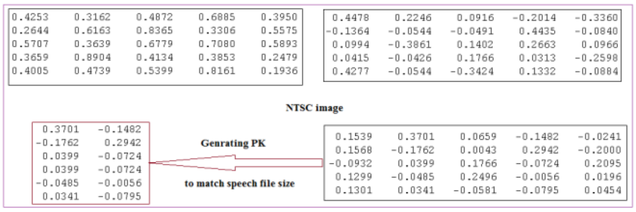
49	178	127	168	185
174	96	229	87	79
77	219	210	74	214
138	218	164	87	145
38	151	209	136	94

242	194	103	15
155	5	234	207
227	113	228	35

52	4	214	128
154	113	174	109
51	119	212	48

49	178	168	185
77	219	74	214
38	151	136	94

Figure 4. Private key generation for image encryption



0.4253	0.3162	0.4872	0.6885	0.3950
0.2644	0.6163	0.8365	0.3306	0.5575
0.5707	0.3639	0.6779	0.7080	0.5893
0.3659	0.8904	0.4134	0.3853	0.2479
0.4005	0.4739	0.5399	0.8161	0.1936

0.4478	0.2246	0.0916	-0.2014	-0.3360
-0.1364	-0.0544	-0.0491	0.4435	-0.0840
0.0994	-0.3861	0.1402	0.2663	0.0966
0.0415	-0.0426	0.1766	0.0313	-0.2598
0.4277	-0.0544	-0.3424	0.1332	-0.0884

0.3701	-0.1482
-0.1762	0.2942
0.0399	-0.0724
0.0399	-0.0724
-0.0485	-0.0056
0.0341	-0.0795

0.1539	0.3701	0.0659	-0.1482	-0.0241
0.1568	-0.1762	0.0043	0.2942	-0.2000
-0.0932	0.0399	0.1766	-0.0724	0.2095
0.1299	-0.0485	0.2496	-0.0056	0.0196
0.1301	0.0341	-0.0581	-0.0795	0.0454

Figure 5. Private key generation for speech encryption

The proposed method can be used to encrypt and data applying the following steps:

1) *Get the image-key.*
2) *Select the data to be encrypted.*
3) *Get the data size.*
4) *If the data is speech file skip to step 8*
5) *Resize the image-key to match the data size*
6) *Apply XORing to get the encrypted data*
7) *Exit*
8) *Convert the image-key to NTSC image.*
9) *Resize the NTSC image to match the speech file size*
10) *Add the resized image to the speech file to get the encrypted data.*

The decryption phase can be implemented applying the following steps:

1) *Get the image-key.*
2) *Select the encrypted data size.*
3) *Get the encrypted data size.*
4) *If the data is speech file skip to step 8*
5) *Resize the image-key to match the data size*
6) *Apply XORing to get the encrypted data*
7) *Exit*
8) *Convert the image-key to NTSC image.*
9) *Resize the NTSC image to match the speech file size*
10) *Subtract the resized image from the encrypted speech file to get the decrypted data.*

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed method was implemented using various SM with varying the message size, a mat lab code was written to implement the proposed method using PC with 5i processor, 2.4 G hertz, and 8 G Byte memory, the other methods of data cryptography were also implemented. Table 2 shows the obtained experimentally encryption time for each method.

Text file with sizes up to 1 M bytes were taken and encrypted-decrypted using the proposed method and the related methods. Table 3 shows the obtained experimental results.

Different color images with various sizes were taken and encrypted-decrypted using the proposed method and the related ones; Figure 6 shows a sample output of running the proposed method, while Table 4 shows the encryption time for each image.

10 speech signals were taken and encrypted-decrypted using the proposed method and the other related ones; Figure 7 shows a sample output of the proposed method, while Table 5 shows the encryption time for the implemented methods.

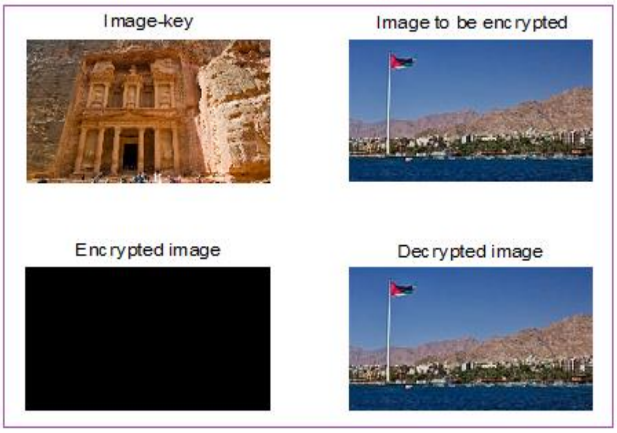


Figure 6. Sample outputs of the proposed method

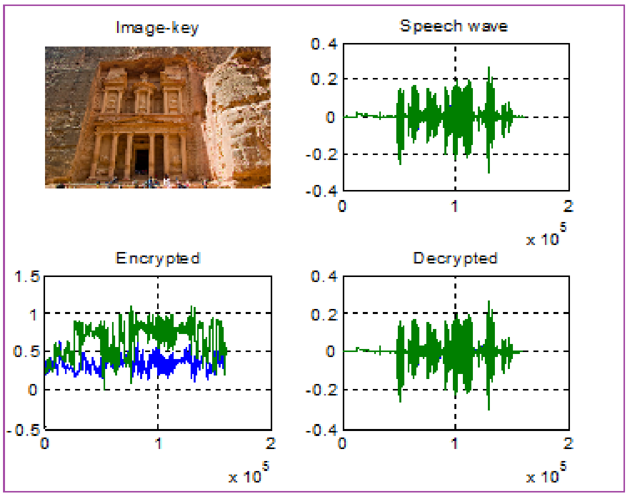


Figure 7. Sample speech encryption-decryption using proposed method

All the related methods gave good results for MSE and PSNR during the encryption phase, while MSE was equal 0 and PSNR equal infinite for the decrypted data.

The proposed method also gave good results for the parameters MSE and PSNR during the encryption phase, while MSE was always equal zero and PSNR equal infinite during the decryption phase, Table 6 shows the values of MSE and PSNR for the encrypted-decrypted images.

Table 2. Encryption time for SM

M. length (character)	DES (1)	3DES (2)	AES (3)	RC2 (4)	RC6 (5)	Blow fish (6)	Proposed (7)
10	0.0000024	0.0028	0.0000023	0.0029	0.00000133	0.00000037	0.000004
50	0.0000119	0.0138	0.0000114	0.0147	0.00000663	0.00000184	0.000004
100	0.0000238	0.0276	0.0000228	0.0294	0.00001326	0.00000368	0.000004
150	0.0000357	0.0415	0.0000343	0.0441	0.00001990	0.00000552	0.000004
200	0.0000476	0.0553	0.0000457	0.0587	0.00002653	.00000737	0.000004
250	0.0000595	0.0691	0.0000571	0.0734	0.00003316	.00000921	0.000004
300	0.0000713	0.0829	0.0000685	0.0881	0.00003979	.00001105	0.000004
350	0.0000832	0.0967	0.0000800	0.1028	0.00004642	.00001289	0.000004
400	0.0000951	0.1106	0.0000914	0.1175	0.00005306	.00001473	0.000004
450	0.0001070	0.1244	0.0001028	0.1322	0.00005969	.00001657	0.000004
500	0.0001189	0.1382	0.0001142	0.1469	0.00006632	0.00001842	0.000004
Average time (second)	5.9673e-005	6.9358e-005	5.7318e-005	0.0737	3.3281e-005	9.2409e-006	0.000004
Throughput	4205000	3617600	4377000	3000000	7539000	27152000	62727275
Throughput (M byte per second)	4.0102	3.4500	4.1742	2.8610	7.1898	25.8942	59.8214

Table 3. Encryption time for text files

M. length (K bytes)	DES (1)	3DES (2)	AES (3)	RC2 (4)	RC6 (5)	Blow fish (6)	Proposed (7)
10	0.0023	0.0024	0.0019	0.0026	0.0010	0.0001	0.000028
50	0.0116	0.0122	0.0093	0.0131	0.0052	0.0007	0.000034
100	0.0232	0.0244	0.0187	0.0262	0.0103	0.0015	0.000075
150	0.0348	0.0366	0.0280	0.0393	0.0155	0.0022	0.000091
200	0.0464	0.0489	0.0374	0.0524	0.0207	0.0029	0.000116
250	0.0580	0.0611	0.0467	0.0655	0.0259	0.0037	0.000135
300	0.0696	0.0733	0.0561	0.0786	0.0310	0.0044	0.000167
350	0.0812	0.0855	0.0654	0.0917	0.0362	0.0051	0.000201
400	0.0927	0.0977	0.0747	0.1048	0.0414	0.0059	0.000341
450	0.1043	0.1099	0.0841	0.1179	0.0465	0.0066	0.000371
500	0.1159	0.1222	0.0934	0.1310	0.0517	0.0073	0.000483
1000	0.2319	0.2443	0.1869	0.2620	0.1034	0.0146	0.000855
Average time (second)	0.0727	0.0765	0.0586	0.0821	0.0324	0.0046	0.000241

Table 4. Encryption time for color images

Image size (bytes)	DES (1)	3DES (2)	AES (3)	RC2 (4)	RC6 (5)	Blow fish (6)	Proposed (7)
150849	0.0389	0.0467	0.0395	0.0543	0.0290	0.0096	0.049000
77976	0.0185	0.0216	0.0178	0.0260	0.0103	0.0029	0.040000
518400	0.1233	0.1433	0.1184	0.1728	0.0688	0.0191	0.047000
4326210	1.0288	1.1959	0.9884	1.4421	0.5738	0.1593	0.055000
122265	0.0291	0.0338	0.0279	0.0408	0.0162	0.0045	0.041000
518400	0.1233	0.1433	0.1184	0.1728	0.0688	0.0191	0.041000
150975	0.0359	0.0417	0.0345	0.0503	0.0200	0.0056	0.043000
150975	0.0359	0.0417	0.0345	0.0503	0.0200	0.0056	0.041000
151353	0.0360	0.0418	0.0346	0.0505	0.0201	0.0056	0.041600
1890000	0.4495	0.5224	0.4318	0.6300	0.2507	0.0696	0.042000
6119256	1.4752	1.6915	1.4980	2.2398	0.8917	0.2754	0.050000
Average time (second)	0.3086	0.3567	0.3040	0.4482	0.1790	0.0524	0.0446

Table 5. Encryption time for speech files

Speech size (samples)	DES	3DES	AES	RC2	RC6	Blowfish	Proposed
321536	29.545664	34.3431	28.3846	41.4132	16.4796	4.5757	0.307124
200704	17.018469	19.7818	16.3497	23.8542	9.4923	2.6356	0.268778
227328	19.148779	22.2580	18.3963	26.8402	10.6805	2.9656	0.271926
430080	42.510458	49.4130	40.8400	59.5855	23.7109	6.5835	0.440077
172032	14.597101	16.9673	14.0235	20.4603	8.1418	2.2606	0.211259
133120	11.240491	13.0656	10.7988	15.7554	6.2696	1.7408	0.201458
212992	17.677530	20.5479	16.9829	24.7780	9.8599	2.7377	0.268810
272384	23.044434	26.7862	22.1389	32.3006	12.8534	3.5689	0.296702
47315	7.835670	9.1080	7.5278	10.9830	4.3705	1.2135	0.155618
145408	12.161606	14.1363	11.6837	17.0465	6.7833	1.8835	0.193275
Average time(second)	19.4780	22.6407	18.7126	27.3017	10.8642	3.0165	0.2615

Table 6. Quality parameters for the proposed method

Image #	Size (byte)	MSE	PSNR
1	150849	2.1660e+004	10.9932
2	77976	4.7582e+004	3.1232
3	518400	1.1328e+004	17.4753
4	4326210	2.0381e+004	11.6018
5	122265	1.3296e+004	15.8734
6	518400	1.1423e+004	17.3913
7	150975	2.2027e+004	10.8248
8	150975	1.5904e+004	14.0818
9	151353	1.2780e+004	16.2689
10	1890000	2.4574e+004	9.7307
11	6119256	2.0094e+004	11.7433
12	150849	2.4398e+004	9.8029

Table 7. Methods speedup

Method	DES	3DES	AES	RC2	RC6	Blowfish	Proposed
DES	1.0000	1.1624	0.9607	1.4017	0.5578	0.1549	0.0670
3DES	0.8603	1.0000	0.8265	1.2059	0.4798	0.1332	0.0577
AES	1.0409	1.2099	1.0000	1.4590	0.5806	0.1612	0.0698
RC2	0.7134	0.8293	0.6854	1.0000	0.3979	0.1105	0.0478
RC6	1.7929	2.0840	1.7224	2.5130	1.0000	0.2777	0.1202
Blowfish	6.4571	7.5056	6.2034	9.0508	3.6015	1.0000	0.4329
Proposed	**14.9173**	**17.3395**	**14.3312**	**20.9093**	**8.3203**	**2.3102**	1.0000

Table 8. Methods speedup (Using text files)

Method	DES	3DES	AES	RC2	RC6	Blowfish	Proposed
DES	1.0000	1.1559	0.9851	1.4524	0.5800	0.1698	0.1445
3DES	0.8652	1.0000	0.8523	1.2565	0.5018	0.1469	0.1250
AES	1.0151	1.1734	1.0000	1.4743	0.5888	0.1724	0.1467
RC2	0.6885	0.7959	0.6783	1.0000	0.3994	0.1169	0.0995
RC6	1.7240	1.9927	1.6983	2.5039	1.0000	0.2927	0.2492
Blowfish	5.8893	6.8073	5.8015	8.5534	3.4160	1.0000	0.8511
Proposed	**6.9193**	**7.9978**	**6.8161**	**10.0493**	**4.0135**	**1.1749**	1.0000

5. RESULT ANALYSIS

From the obtained results shown in table we can see that the proposed method has better performance by increasing the short messages encryption process throughput as shown in Figure 8 and the proposed method has a significant speedup comparing with other related method, the speedup can be calculated using Eq. (4).

$$Speedup_{1,2} = \frac{\text{Encryptiontime}_2}{\text{Encryptiontime}_1} \qquad (4)$$

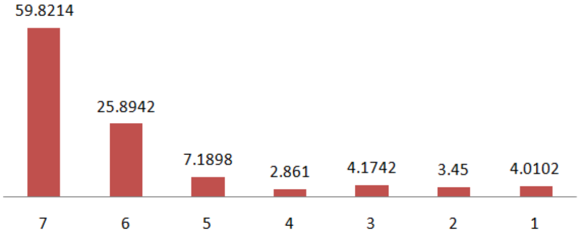


Figure 8. Methods throughputs

Increasing the data size (using text files) will rapidly increase the encryption time for the related method and slowly for the proposed method as shown in Figure 9. Taking the results shown in Table 3 we can calculate the methods speedup, the results of calculations are shown in Table 7.

Using the proposed method to encrypt-decrypt images and speeches also improves the method performance by decreasing the encryption time-decryption times.

The proposed method satisfied the requirements of good method of data cryptography by providing good value for the quality parameters MSE and PSNR (see Table 8).

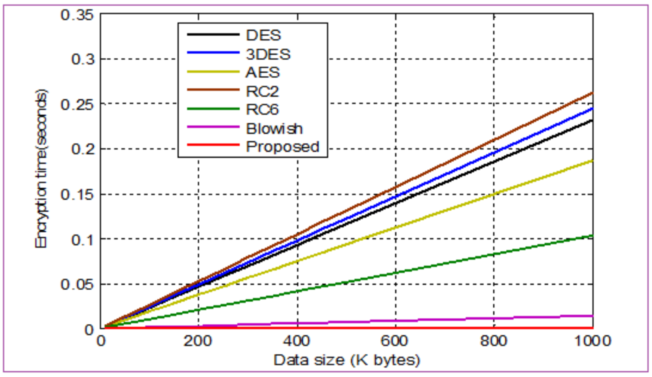


Figure 9. Encryption times comparisons

6. CONCLUSIONS

A simple method of data cryptography was presented. This method can be used encrypt-decrypt short messages, text files, digital images, and digital speeches. The proposed method increases the data security level and provide a highly degree protection based on the use of secrete color image to generate a private key. The proposed method gives very good values of the quality parameters during the encryption and decryption phases. The proposed method was compared with other famous methods of data cryptography and it was shown that the proposed method raises the data cryptography process performance by decreasing the encryption-decryption times, this was proved by the calculated speedup.

REFERENCES

[1] Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098. https://doi.org/10.11591/ijece.v9i5.pp4092-4098

[2] Alqadi, Z. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science, 5(5): 355-362.

[3] Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65. https://doi.org/10.47760/ijcsmc.2021.v10i09.006

[4] Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z. (2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.

[5] Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M., Alqadi, Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-20.

[6] Zaidan, A.A., Majeed, A., Zaidan, B.B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology (WASET), 54: 468-479.

[7] Zaidan, A.A., Zaidan, B.B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. International Journal of Computer and Network Security, 1(1): 1985-1553.

[8] Khalifa, O.O., Naji, A.W., Zaidan, A.A., Zaidan, B.B., Hameed, S.A. (2010). Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput. Sci. Netw. Secur, 9(5): 294-300.

[9] Majeed, A., Mat Kiah, M.L., Madhloom, H.T., Zaidan, B.B., Zaidan, A.A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and Technology, 1(2): 63-69. http://eprints.um.edu.my/id/eprint/4951.

[10] Zaidan, A.A., Othman, F., Zaidan, B.B., Raji, R.Z., Hasan, A.K., Naji, A.W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering, 1: 1-7.

[11] Aos, A.Z., Naji, A.W., Hameed, S.A., Othman, F., Zaidan, B.B. (2009). Approved undetectable-antivirus steganography for multimedia information in PE-file. In 2009 International Association of Computer Science and Information Technology-Spring Conference, pp. 437-444. https://doi.org/10.1109/IACSIT-SC.2009.103

[12] Zaidan, A.A., Zaidan, B.B., Abdulrazzaq, M.M., Raji, R.Z., Mohammed, S.M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 19: 482-489.

[13] Naji, A.W., Zaidan, A.A., Zaidan, B.B., Muhamadi, I.A. (2010). Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET), 56(5): 498-502.

[14] Abomhara, M., Zakaria, O., Khalifa, O.O., Zaidan, A.A., Zaidan, B.B. (2022). Enhancing selective encryption for H. 264/AVC using advanced encryption standard. International Journal of Computer and Electrical Engineering (IJCEE), 2(2): arXiv:2201.03391. https://doi.org/10.48550/arXiv.2201.03391

[15] Naji, A.W., Hameed, S.A., Zaidan, B.B., Al-Khateeb, W.F., Khalifa, O.O., Zaidan, A.A., Gunawan, T.S. (2009). Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. International Journal of Computer Science and Information Security (IJCSIS), 3(1): 73-78. arXiv:0908.0216.

[16] Hamdan, A., Jalab, H.A., Zaidan, A.A., Zaidan, B.B. (2010). New frame work of hidden data with in non multimedia file. Int. J. Comput. Netw. Secur, 2(1): 46-54.

[17] Taqa, A., Zaidan, A.A., Zaidan, B.B. (2009). New framework for high secure data hidden in the MPEG using AES encryption algorithm. International Journal of Computer and Electrical Engineering, 1(5): 1793-8163.

[18] Zaidan, A.A., Zaidan, B.B., Jalab, H.A. (2010). A new system for hiding data within (unused area two+ image page) of portable executable file using statistical technique and advance encryption Standared. International Journal of Computer Theory and Engineering, 2(2): 218.

[19] Ignatiev, A., Morgado, A., Marques-Silva, J. (2019). RC2: An efficient MaxSAT solver. Journal on Satisfiability, Boolean Modeling and Computation, 11(1): 53-64.

[20] Verma, P., Shekhar, J., Preety, A.A. (2015). A survey for performance analysis various cryptography techniques digital contents. International Journal of Computer Science and Mobile Computing, 4(1): 522-531. https://doi.org/10.3233/SAT190116

[21] Alanazi, H., Zaidan, B.B., Zaidan, A.A., Jalab, H.A., Shabbir, M., Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. Journal of Computing, 2(3). arXiv:1003.4085.

[22] Thakur, J., Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International Journal of Emerging Technology and Advanced Engineering, 1(2): 6-12.