IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

Replaced ASCII table to encode-decode secret messages

Hatim Ghazi Zaini

Department of computer Engineering, Taif University, Taif, KSA

Abstract: Messages are circulated very widely through social media, and some of these messages may be confidential or have a personal character, which requires protection of this type of messages from people who are intrusive or have nothing to do with the message. In this paper, we will discuss a new method for encoding short and long text messages, which depends on the use of a special table modified for ASCII table, which includes the locations of the different symbols in a specific image. The proposed method is based on the use of the modified table, noting that `this schedule changes from one image to another, which makes the process of understanding the encrypted text message impossible. The proposed method will be implemented and tested, and the obtained experimental results will be evaluated to show the efficiency and reliability of the proposed method.

Key words: Digital image, secret message, ASCII table, Updated table, encryption, decryption, throughput, efficiency, reliability.

I- INTRODUCTION

A short or long text message [4] is a set of symbols represented by ASCII table with fixed and specific values [17], [18] that are circulated between two people through social media. The text message may [31], [32] be of a personal nature as it contains personal information or it may contain confidential information that no third party has the right to view or hack into [1], [2], [3].
Currently [19], [20], many methods are used to encrypt-decrypt text messages, and some of these methods are based on international standards DES and AES and some of them depend on the exclusion or multiplication process [4]. [5]. [6].
Color digital images [7], [8] are one of the most prevalent types of data due to the many vital applications [9], [10] that use this group of data for several reasons, the most important of which are:

- Ease of getting the digital image at no cost [11], [12].
- Ease of processing [13], [14].
- High resolution, which provides a huge volume of data which can be used for multiple purposes [15], [16].

The digital color image is represented by a three-dimensional matrix [21], [22], where each of the three dimensions is assigned to a color (the first for red, the second for green, and the third for blue) [23], [24]. The point values in each color matrix range from 0 to 255 and these values cover the values in the ASCII table used to encode the different symbols that can constitute the secret message.
Here in this paper research we will introduce a new approach of message securing by using that uses the locations of the values between 0 and 255 to form a new updated table, which can be used to re-encode the secret message and generate the encrypted secret message [25], [26].
Before using color image to create the updated table, we have to sure that the image contains all the values between 0 and 255, this can be done by replacing 256 pixels in the image with these value, the replacement will not affect the image much, as shown in figures 1 and 2 [27], [28].

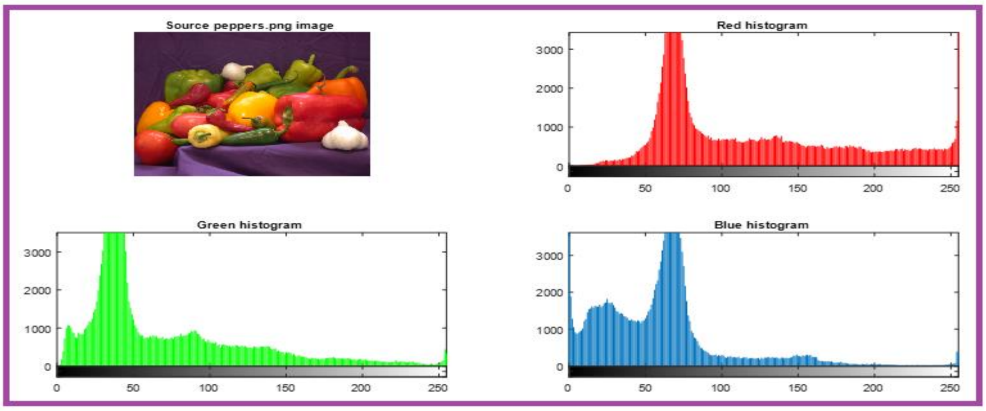


Figure 1: Sample of the color image

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

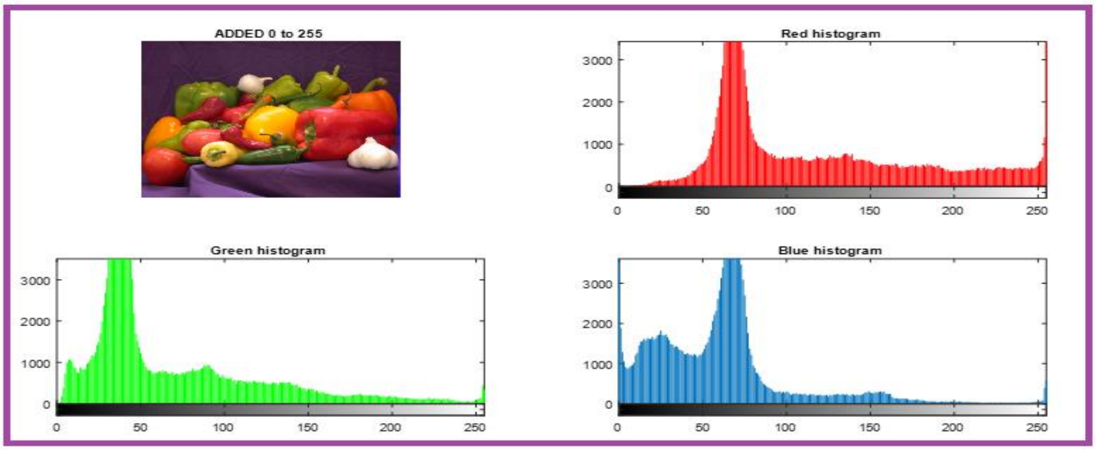


Figure 2: Image after replacing the values of 256 pixels

II- THE PROPOSED METHOD

The high security level and secret message [29], [32] protection of proposed method can be achieved by selecting a color image to be used to generate the updated table as shown in figure 3. The selected message is an agreed image between the sender and receiver and it will be available to both of them and there is no need to send it, also the selected source image can be changed whenever the sender and receiver decide to do this.

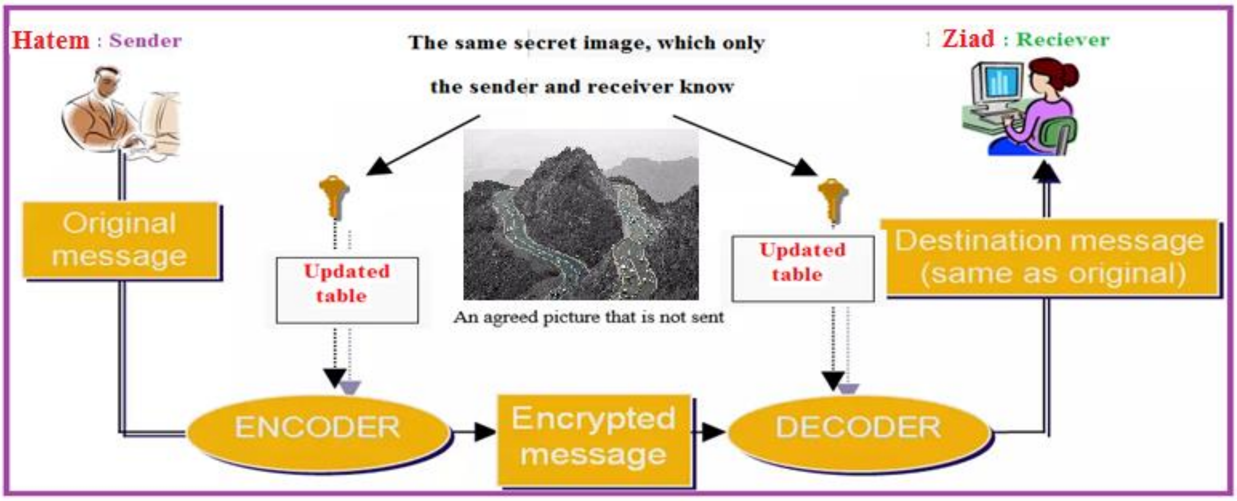


Figure 3: Proposed method diagram

The proposed method can be implemented applying the following steps:

Encryption phase:

1) Get the source image.
2) Get the image size.
3) Reshape the image into one row matrix.
4) Check whether the row matrix contains all the values between 0 and 255, if not replace some pixels in the image with the required missing values.
5) For each value in the ASCII table find the first location in the image that contains the ASCII value and store it in the updated table.
6) Get the secret message, and get the message length.
7) For each character in the massage find the associated location in the updated table, and add it to the encrypted message.
8) Send the encrypted message.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

Decryption phase

This phase can be implemented applying the following steps:

1) Get the source image.
2) Get the image size.
3) Reshape the image into one row matrix.
4) Check whether the row matrix contains all the values between 0 and 255, if not replace some pixels in the image with the required missing values.
5) For each value in the ASCII table find the first location in the image that contains the ASCII value and store it in the updated table.
6) Get the encrypted message, and get the message length.
7) For each value in the massage find the index associated with the location to get the ASCII code, add this code to the decrypted message.

III- IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed method was implemented using matlab; figure 4 shows the ASCII table, while table 1 shows the obtained updated table using the peppers.png image as a source image:

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Figure 4: ASCII table

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

Table 1: Updated table

0	397314	31	9955	62	10	93	693	124	367	155	2586	186	2978	217	4901	248	8724
1	213091	32	**22630**	63	**1(A)**	94	1469	125	375	156	1444	187	2977	218	4900	249	9107
2	211555	33	8802	64	**2(B)**	95	692	126	368	157	1452	188	2592	219	5272	250	10639
3	206559	34	20323	65	**16(C)**	96	357	127	372	158	2222	189	2588	220	5274	251	11024
4	206176	35	8803	66	**3(D)**	97	**680(a)**	128	373	159	1836	190	2591	221	5280	252	11414
5	32224	36	1807	67	**31(E)**	98	**1082(b)**	129	370	160	1824	191	3363	222	5277	253	11417
6	32223	37	2960	68	24	99	**1125(c)**	130	1462	161	1445	192	2590	223	5275	254	11798
7	26852	38	1422	69	30	100	**1081(d)**	131	371	162	1446	193	2589	224	5276	255	12181
8	24549	39	1037	70	25	101	**691(e)**	132	378	163	1449	194	3745	225	5656		
9	27235	40	270	71	57	102	**681(f)**	133	1847	164	1450	195	3358	226	5658		
10	24165	41	272	72	116	103	1080	134	1073	165	1447	196	2974	227	5659		
11	24933	42	653	73	93	104	1127	135	1063	166	1833	197	2970	228	6038		
12	26084	43	247	74	115	105	**1060**	136	2231	167	4099	198	2973	229	6040		
13	28002	44	268	75	117	106	358	137	1072	168	1825	199	2971	230	5664		
14	23013	45	263	76	107	107	359	138	2230	169	2217	200	3739	231	6042		
15	23397	46	248	77	133	108	1130	139	1460	170	2602	201	3352	232	6045		
16	24932	47	260	78	242	109	360	140	1064	171	1826	202	3354	233	6046		
17	22629	48	644	79	294	110	361	141	1065	172	1829	203	4124	234	6422		
18	24164	49	249	80	295	111	684	142	1071	173	1827	204	3353	235	6428		
19	22245	50	630	81	108	112	384	143	1070	174	1831	205	4515	236	6430		
20	21861	51	257	82	297	113	1078	144	1066	175	1828	206	3734	237	6811		

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

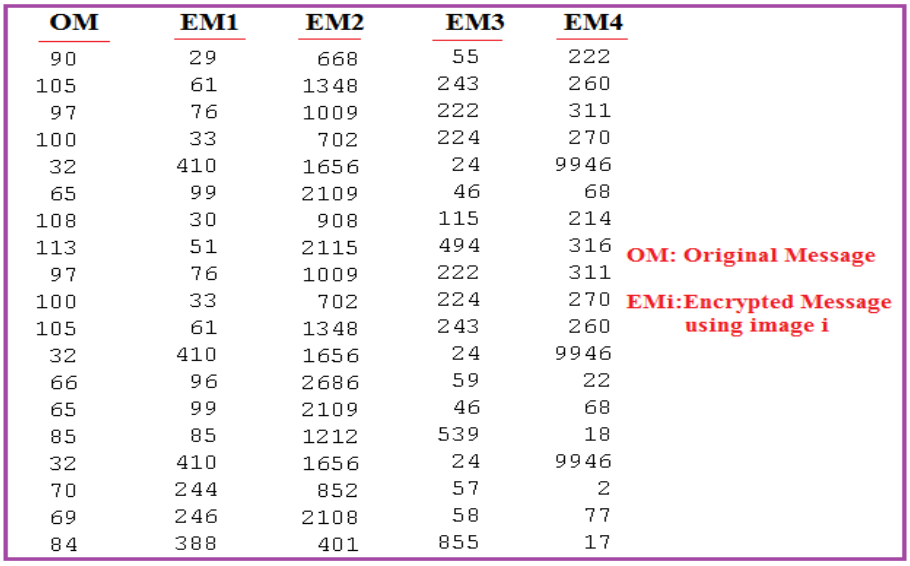
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

21	24550	52	250	83	110	114	383	145	1067	176	2214	207	4505	238	6806	
22	21477	53	256	84	298	115	768	146	1068	177	2213	208	3735	239	6805	
23	21093	54	634	85	305	116	747	147	3383	178	2587	209	4118	240	6808	
24	20709	55	638	86	302	117	750	148	1842	179	2599	210	4119	241	7190	
25	20325	56	220	87	303	118	362	149	1823	180	2206	211	4502	242	7576	
26	9186	57	14	88	304	119	766	150	1443	181	3759	212	4500	243	7573	
27	21476	58	11	89	355	120	365	151	1840	182	2210	213	4501	244	7574	
28	20324	59	17	90	**1105**	121	363	152	2224	183	2595	214	4884	245	8342	
29	9571	60	27	91	333	122	1076	153	4154	184	2207	215	5650	246	8341	
30	9570	61	9955	92	356	123	366	154	1455	185	2208	216	4891	247	8340	

As we said, the source image can be changed, and here the encrypted versions for the same secret message will be different as shown in figure 5:



OM	EM1	EM2	EM3	EM4
90	29	668	55	222
105	61	1348	243	260
97	76	1009	222	311
100	33	702	224	270
32	410	1656	24	9946
65	99	2109	46	68
108	30	908	115	214
113	51	2115	494	316
97	76	1009	222	311
100	33	702	224	270
105	61	1348	243	260
32	410	1656	24	9946
66	96	2686	59	22
65	99	2109	46	68
85	85	1212	539	18
32	410	1656	24	9946
70	244	852	57	2
69	246	2108	58	77
84	388	401	855	17

OM: Original Message

EMi:Encrypted Message using image i

Figure 5: Different encrypted messages using different images

Here we have to notice that using any color image as a source one we can encrypt-decrypt messages with variable length, and the message length can be unlimited. The following image shown in figure 6 was taken as a source image, various messages were encrypted-decrypted using this image, the encryption and decryption times were measured, table 2 shows the obtained experimental results:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

Figure 6: Source image (image size=150849 bytes)

Table 2: Obtained results

Message length	Encryption time(Second)	decryption time (Seconds)	Throughput
19	0.270000	0.270000	70
32	0.274000	0.274000	120
52	0.281000	0.281000	190
104	0.296000	0.296000	350
208	0.302000	0.302000	690
416	0.309000	0.309000	1350
1664	0.370000	0.370000	45000
6656	0.385000	0.385000	17290
53248	0.515000	0.515000	103390
212992	1.834000	2.834000	116140

From the obtained results shown in table 2 we can raise the following facts:
- The secret message length can be bigger than the image size.
- We can use any color image as a source image to encrypt-decrypt the secret message.
- The proposed method is very flexible by changing the source image whenever we want.
- There is no need to send the source image, it must be kept in secret by both the sender and receiver, and thus we can achieve a high level of security.
- The proposed method is very efficient by providing a small encryption-decryption time, thus the providing method maximizes the method throughput (number of encrypted/decrypted bytes per second). See figures 7 and 8.
- The proposed method is very simple to be implemented

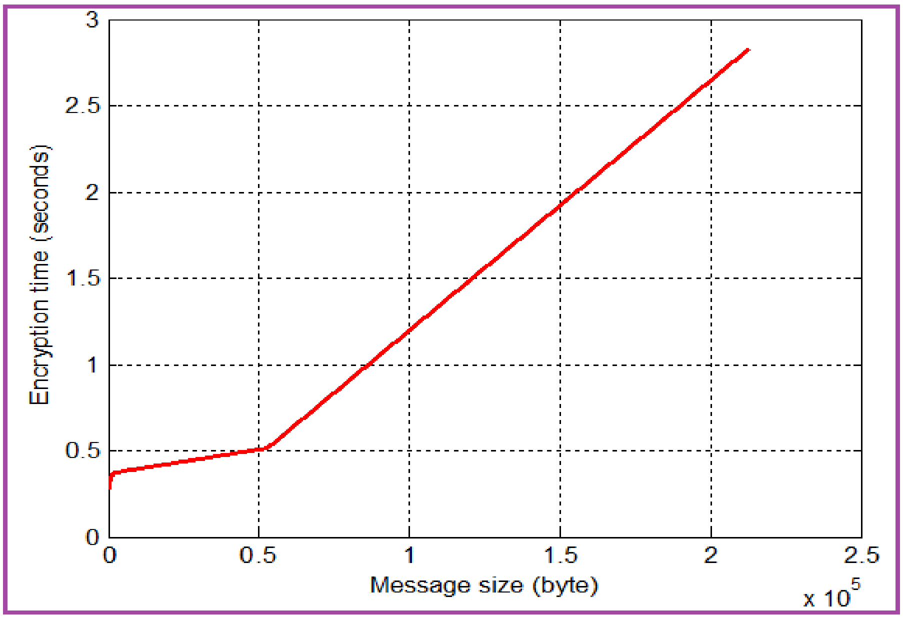


Figure 7: Relationship between message length and encryption time

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

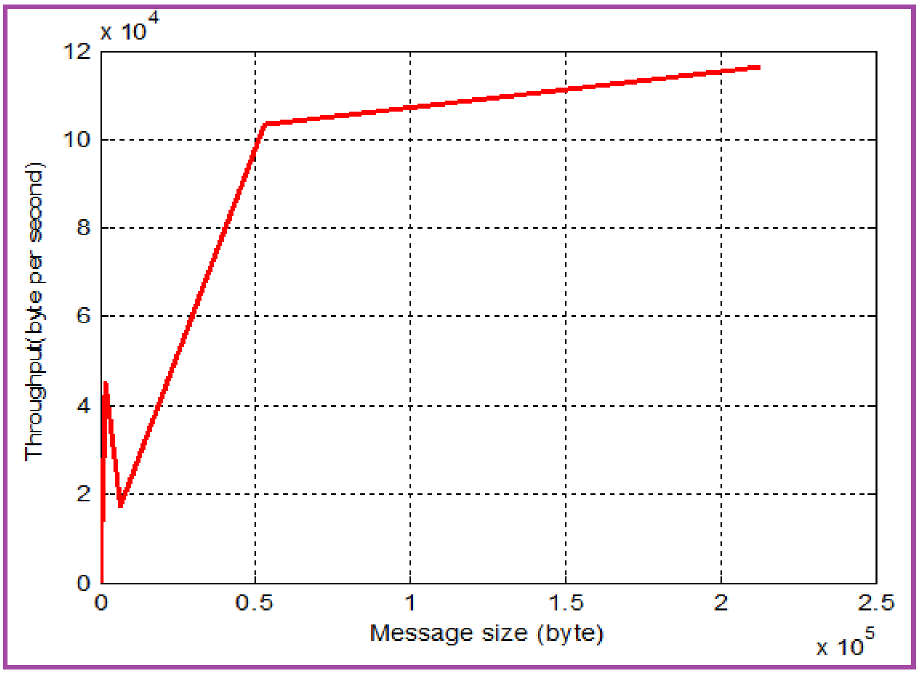


Figure 8: Relationship between message length and method throughput

For messages with KB sizes, the throughput was compared with DES and AES results [33] and the proposed method gave better results by raising the throughput from 4.4 to 116 Kb per second.

IV-Conclusion

A method of secret message encryption-decryption was proposed, tested and implemented. This method is based on replacing the ASCII table by a new updated table which contains the first occurrence (location) of the ASCII symbol in the source image.

The proposed method has a high level of security, this can be achieved by keeping the source image unknown (secret) to any third party, and by selecting an image with huge size, also there is a possibility to change the source image from time to time.

The experimental results showed that the proposed method is very efficient by maximizing the method throughput

REFERENCES

[1] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.
[2] Ziad AlQadi, M Elsayyed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017.
[3] Ziad AlQadi, analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[4] Prof. Yousif El Tous Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Message segmentation and image blocking to secure data steganography, International Journal of Computer Science and Mobile Computing, vol. 9, issue 8, pp.75-82, 2020.
[5] Belal Zahran Rashad J. Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, Developing new multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp.3228-3235, 2020.
[6] Dr. Majed Omar Dwairi Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Simple and Highly Secure, Efficient and Accurate Method (SSEAM) to Encrypt-Decrypt Color Image, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 4, pp. 64-69, 2020.
[7] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
[8] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A Alqadi, Mohammad Khalil Abuzalata, Creating a Color Map to be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, pp. 31-34, 2016.
[9] Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.
[10] Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using Matlab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 21-28, 2016.
[11]Mazen A.Hamdan Bassam M.Subaih, Prof. Ziad A. Alqadi, Extracting Isolated Words from an Image of Text, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 29-36, 2016.
[12] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.
[13]Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10314

[14] Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.

[15]Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[16] Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319,2020.

[17] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[18]Ziad AlQadi, M Elsayyed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017.

[19] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[20]Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[21]Ayman Al-Rawashdeh, Ziad Al-Qadi, Using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[22]Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[23]ZIAD ALQADI, A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES, Journal of Theoretical and Applied Information Technology, vol. 96, issue 10, pp. 3014-3024,2018.

[24]Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780-2787, 2018.

[25]Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[26]Ahmad Sharadqh Jamil Al-Azzeh , Rashad Rasras , Ziad Alqadi , Belal Ayyoub, Adaptation of matlab K-means clustering function to create Color Image Features, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 2, pp. 10-18, 2019.

[27] Yousf Eltous Ziad A. AlQadi, Ghazi M. Qaryouti, Mohammad Abuzalata, ANALYSIS OF DIGITAL SIGNAL FEATURES EXTRACTION BASED ON KMEANS CLUSTERING, International Journal of Engineering Technology Research & Management, vol. 4, issue 1, pp. 66-75, 2020.

[28]Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, Creating Human Speech Identifier using WPT, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 117-123, 2020.

[29]Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.

[30] Dr. Amjad Hindi, Dr. Ghazi M. Qaryouti, Prof. Yousif Eltous, Prof. Mohammad Abuzalata, Prof. Ziad Alqadi, Color Image Compression using Linear Prediction Coding, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 13 – 20, 2020.

[31] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi,A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.

[32] Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.

[33] Shaza D. Rihan, A h m e d Khalid, Saife Eldin F. Osman, A Performance Comparison of Encryption Algorithms AES and DES, International Journal of Engineering Research & Technology (IJERT), vol. 4, issue 12, pp. 151-154, 2015.