An Image Encryption & Decryption And Comparison With Text - AES Algorithm

Dr. N. Suba Rani, Dr. A. Noble Mary Juliet, K. Renuka Devi

Abstract: With the advent of internet technology, the number of unauthorized users to access the data increases.so, the transmission of information through image becomes more. And it also becomes more reliable form to transmit data. There are number of algorithms available to solve this problem. One of the efficient method is to use AES (Advanced Encryption Standard) algorithm, the most notable and extensively used cryptographic algorithm because it is six times faster than 3-DES and much faster than RSA algorithm. In this paper we proposed an image encryption and decryption algorithm using AES in which encryption contains a random image and decryption contains original image. The algorithm is implemented in java. The efficiency of AES is compared using image and text and it is analyzed. The result thus shows that the sharing of information through image is much more reliable and efficient than sharing information as text.

Index Terms: AES, Cryptography, Decryption, Encryption, Image.

1 INTRODUCTION

EVERY cryptographic process has two aspects: the algorithm and the key used for the encryption and decryption [1]. The use of the keys makes the cryptographic process reliable. There are two types of cryptographic mechanisms: Symmetric key cryptography - uses same key for encryption and decryption process. Asymmetric key cryptography - uses two different keys for encryption and decryption process. Symmetric key algorithm is efficient, fast and easy to implement as compared to asymmetric key algorithm. The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. AES is a symmetric block cipher and it is believed to be the standard process, So, it replaces DES algorithm in most number of applications[1]. When compared to other symmetric and public key ciphers, the AES symmetric cipher is found to be complex.

2 ADVANCED ENCRYPTION STANDARD

2.1 AES – PROCESS

The characteristics of AES algorithm are given below −

- Uses common (Symmetric) key and so, it is called as Symmetric block cipher.
- The size of data is 128 bits, and so the key size varies from 128/192/256 bits.
- It is highly robust and 6 times faster than 3-DES and much faster and powerful than RSA.
- It uses single S-box for all rounds rather than DES, where it uses eight S-boxes.

- ***Dr. N. Suba Rani**, Assistant Professor(SG), Department of computer Science, Dr.Mahalingam College of Engineering and Technology, Tamilnadu, India, suba@drmcet.ac.in,9994721111.*
- ***Dr. A. Noble Mary Juliet** Associate Professor, Department of computer Science, Dr.Mahalingam College of Engineering and Technology, Tamilnadu, India*, cse.julie@drmcet.ac.in, 9791534556.
- ***K. Renuka Devi**, is currently pursuing her Master's degree program in Department of computer Science, Dr.Mahalingam College of Engineering and Technology, Tamilnadu, India, krenukagiri@gmail.com, 8838088448.*

The process involved in AES is iterative when compared with Fiestel cipher. AES is generally based on Substitution and Permutations operations. It consists of sequence of linked operations at each round. Each round consists of the following process. 1) Interchanging of inputs by the outputs produced by the substitution process. 2) The bits are shifted in a cyclic manner. 3) The columns are mixed by transformation. 4) The key has been added with input using XOR operation. The computation of AES is performed at bytes level, so 128 bits of plain-text is considered as a block of 16 bytes which constitute a 4x4 matrix. Each round of AES depends on the key length. AES performs 10/12/14 rounds depending on the key size 128/192/256 respectively. So, AES is known to be AES-128, AES-192 and AES-256 algorithm based on key size. A unique 128 bit round key is given as an input at each round [2].

2.2 AES – Encryption and Decryption Specification

AES is called AES-128, AES-192 and AES-256. This classification depends on the different key size used for cryptographic process. Those different key sizes are used to increase the security level. As, the key size increases the security level increases. Hence, key size is directly proportional to the security level. The input for AES process is a single block of 128 bits. The processing is carried out in several number of rounds where it depends on the key length: 16 byte key consists of 10 rounds, 24 byte key consists of 12 rounds, and 32 byte key consists of 14 rounds. The first round of encryption process consists of four distinct transformation functions:

- Substitution Bytes
- ShiftRows
- MixColumns
- AddRoundKey

The final round consists of only three transformation ignoring MixColumns. The Decryption method is the reverse of encryption and it consists of four transformations [4].

- Inverse Substitution Bytes
- Inverse ShiftRows
- Inverse MixColumns
- AddRoundKey

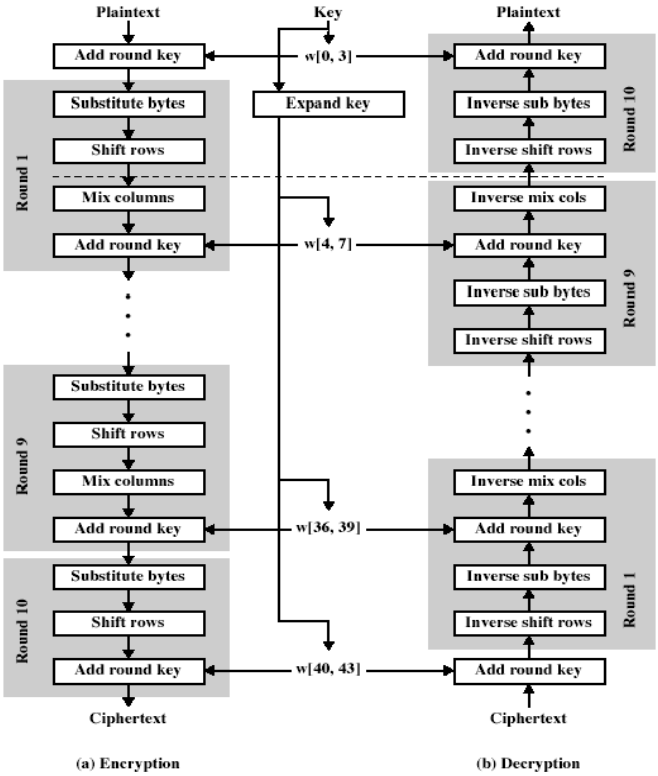


Fig 1. *Process of AES Encryption and Decryption*

Table I. *AES-parameters*

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

2.3 AES – Encryption process

2.3.1 Substitution bytes:

The 16 byte plain-text substitutes the corresponding value from substitution table S-box [8]. It is a non-linear method which performs in the following way:

Table II. *S-Box*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

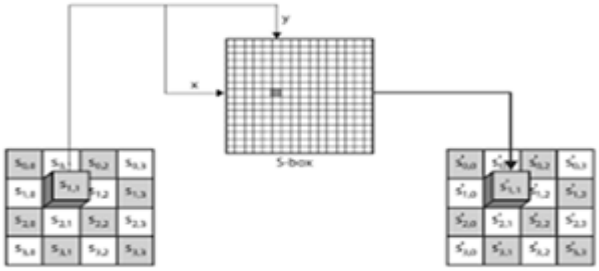


Fig 2. Substitution bytes – process

2.3.2 ShiftRows:

In shiftrows transformation, the bytes in last 3 rows will be shifted cyclically over number of bytes present.

- The first row will remain same.
- The second row will get shifted to the left by one position.
- The third row will get shifted to the left by two positions.
- The fourth row will be shifted to the left by three positions.

Resulting matrix consists of same 16 bytes but shifts with one another.

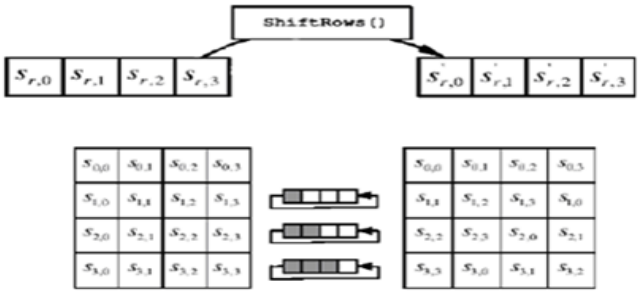
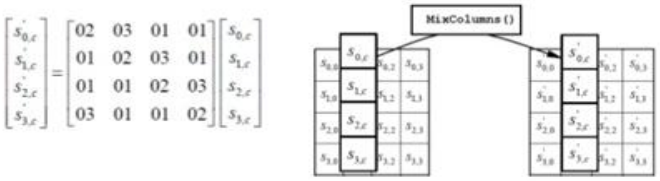


Fig 3. *ShiftRows-process*

2.3.3 MixColumns:

MixColumns transformation performs by transforming each column of four bytes. It takes input as one column which is of 4 bytes and output as completely different 4 bytes by transforming the original column. The resultant matrix is same as the size of plain-text. MixColumn transformation will not be carried in the last round.



$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

Fig 4. *MixColumns-Process*

2.3.4 AddRoundKey:

The 16 bytes which is produced from MixColumns is equal to 128 bits which is XORed with the round key of 128 bits. The above process has been repeated until final round to produce the corresponding cipher text [5].

$$b(i, j) = a(i, j) \oplus k(i, j) \quad (1)$$

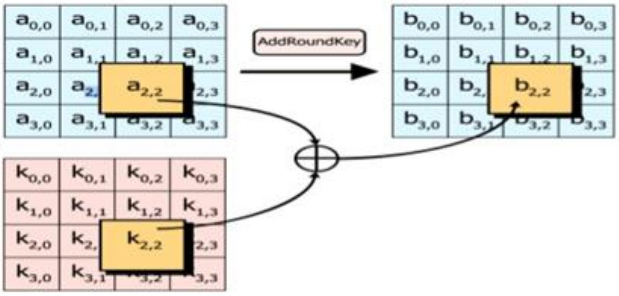


Fig 5. *AddRoundKey-Process*

2.4 AES – DECRYPTION PROCESS

2.4.1 Inverse Substitution Bytes:

Inverse Substitution Bytes is the inverse of the substitution byte transformation. This is performed through inverse S-box [6,7]. This is obtained by applying inverse of substitution bytes and by computing multiplicative inverse of Galois Field - GF (2^8).

Table III. *Inverse S-Box*

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

2.4.2 Inverse ShiftRows:

Inverse ShiftRows is the inverse of ShiftRows transformation. It carries out circular shifts in reverse direction for each last 3 rows and for the 2nd row, it performs one-byte circular shift to the right and it continues the process till (n-3)rd row.

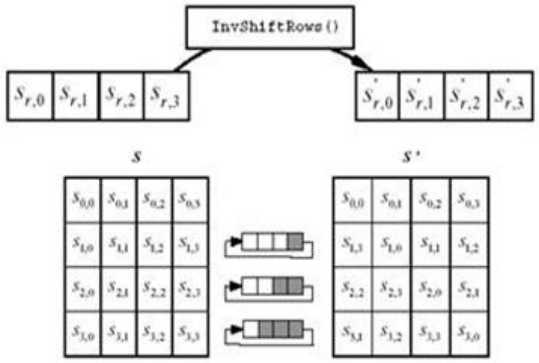


Fig 6. *Inverse ShiftRows-Process*

2.4.3 Inverse MixColumns:

Inverse MixColumns is the inverse of Mixcolumns transformation. It carries out operations on a matrix by column-wise. Resultant columns are in the form of polynomials.

$$a^{-1}(x)=\{0B\}x^3 \oplus \{0D\}x^2 \oplus \{09\}x \oplus \{0E\}$$

$s'(x) = a^{-1}(x) \otimes s(x)$:

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb.$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

$$s'_{0,c} = (\{0e\} \bullet s_{0,c}) \oplus (\{0b\} \bullet s_{1,c}) \oplus (\{0d\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c})$$

$$s'_{1,c} = (\{09\} \bullet s_{0,c}) \oplus (\{0e\} \bullet s_{1,c}) \oplus (\{0b\} \bullet s_{2,c}) \oplus (\{0d\} \bullet s_{3,c})$$

$$s'_{2,c} = (\{0d\} \bullet s_{0,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0e\} \bullet s_{2,c}) \oplus (\{0b\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{0b\} \bullet s_{0,c}) \oplus (\{0d\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0e\} \bullet s_{3,c})$$

Fig 7. *Inverse ShiftRows-Process*

3 IMPLEMENTATION

3.1 AES-Encryption algorithm

The implementation of AES-encryption is done in java. The input given to the encryption process is a Plain-text (or) a Plain-image. The image is divided into 4*4 matrix and so there are 10 rounds performed for this process. So, there are totally nine rounds performed with 4 transformations (i.e.) subbytes, shiftrows, mixcolumns and addroundkey. And 10th round consists of three transformations ignoring Mixcolumns [9,10]. The original image will be encrypted and the encrypted image will be displayed as another random image to the sender. This encryption process also applied on text and the encryption process is same and the result is obtained.

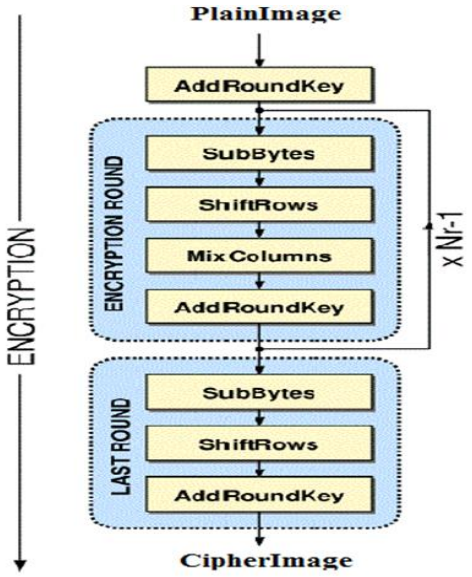


Fig 8. *AES – Encryption process*

3.2 AES-Decryption algorithm

The AES decryption is an inverse of encryption process. The below figure shows the decryption process. The decryption process takes the cipher-image (or) cipher-text as input and it performs the four transformations (i.e.) Inverse subbytes, Inverse Shiftrows, Inverse Mixcolumns and Addroundkey until 9 rounds and the 10th round performs three transformation ignoring Inverse Mixcolumns [11]. The output of decryption process will produce the original image to the receiver.

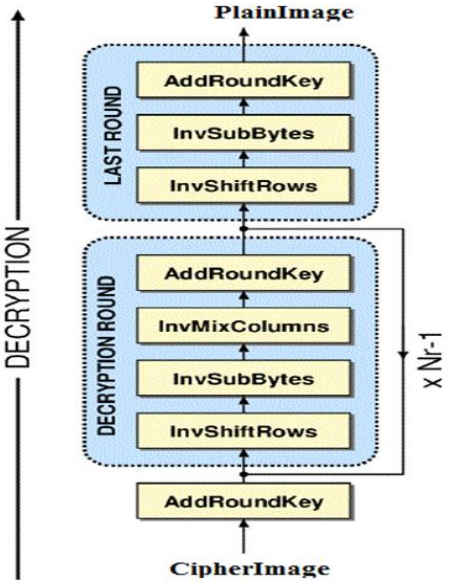


Fig 9. *AES-Decryption Process*

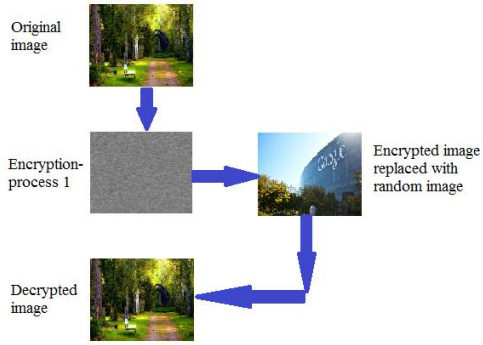


Fig 10. *System Process*

4 RESULTS

4.1 Image

The input-image given to the AES algorithm is of JPG/PNG format. The original image is given to the encryption process, produced the cipher-image and decryption process is enhanced by providing the cipher-image as input, produced the plain-image. Both encryption and decryption utilize the same key.

Fig 11. *Final Output1*

4.2 Text

The Plain-text is given as input to the AES algorithm, performs the process of encryption, thus produced the cipher-text and the decryption process is enhanced by providing the cipher-text as input, produced the plain-text.

```
Original Text  : hello world
Encrypted Text : s207+VdCkD6p/T9HwcwHGg==
DeCrypted Text : hello world
```

Fig 12. *Final Output2*

5 ANALYSIS

5.1 Text-Time Complexity

The time complexity of encryption and decryption for text has been calculated using AES algorithm and the following results are obtained.

Table IV. *Text-time Complexity*

Size(kb)	Encryption(ms)	Decryption(ms)
20	838	917
25	911	989
50	941	1128
75	1154	1453
100	1704	2117
150	1815	2305

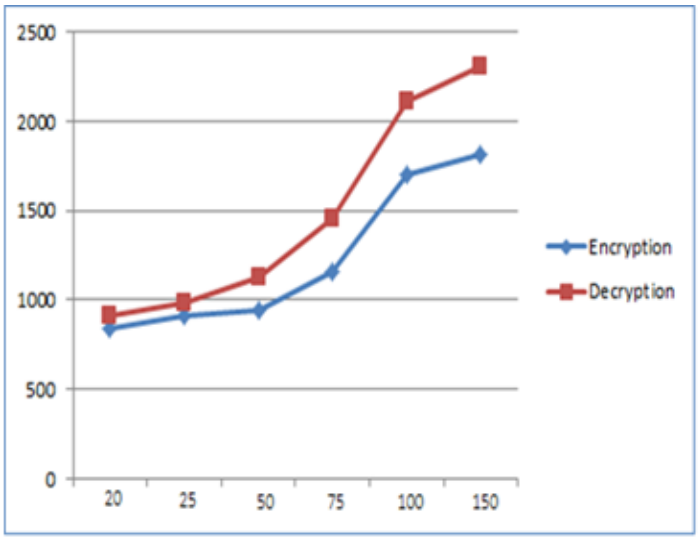


Fig 13. Final Output1

The Table 4 shows the time complexity of text for encryption and decryption. The result conveys that “as the size increases the encryption time increases and decryption time also increases”.

5.2 Image-Time Complexity

The time complexity of encryption and decryption for image has been calculated using AES algorithm and the following results are obtained.

Table V. *Text-time Complexity*

Size(kb)	Encryption(ms)	Decryption(ms)
20	17	25
25	21	34
55	40	58
75	57	98
100	77	132
150	108	188

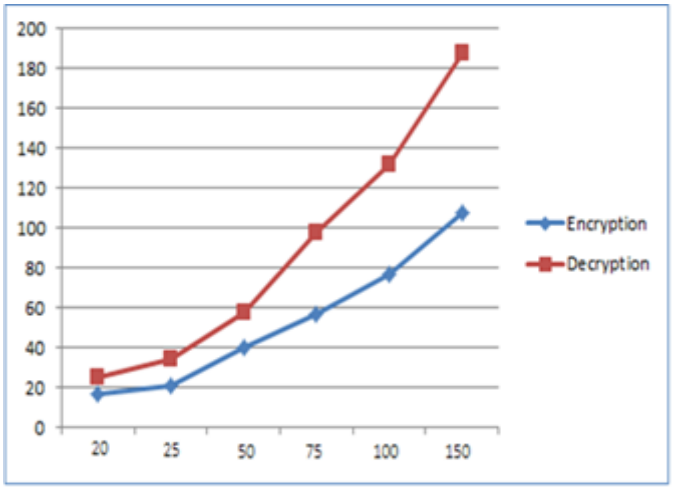


Fig 14. Final Output2

The Table 5 displays the time complexity of image for cryptographic process. The result shows that “as the size increases the encryption time increases and decryption time also increases”. But, to be noted the encryption and decryption time for image is lesser than time complexity of text.

5.3 Comparison-Text & Image

The time complexity of encryption and decryption for both text & image has been compared by using the above results.

Table VI. *Text & Image – Time Complexity*

	Text		Image	
Size (kb)	Encryption (ms)	Decryption (ms)	Encryption (ms)	Decryption (ms)
20	838	917	17	25
25	911	989	21	34
50-55	941	1128	40	58
75	1154	1454	57	98
100	1704	2117	77	132
150	1815	2305	108	188

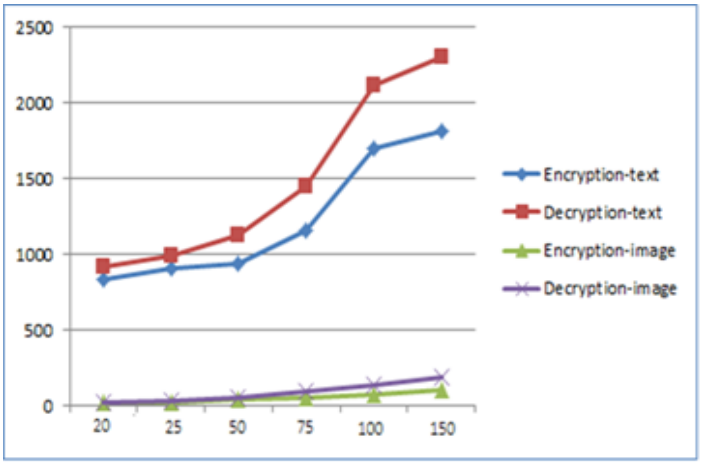


Fig 15. Comparison – Text & Image

6 INFERENCE

- AES algorithm works well for both encryption and decryption.
- From Figure 15 the decryption time is larger than encryption time for both the text and image.
- In Figure 13 and Figure 14 the encryption and decryption time increases with increase in file size.
- But while comparing both text and image from Figure 15 the decryption time of image is lesser than text. So, it is efficient than text.
    - Larger the size, larger the encryption time.
- From above information, AES holds good for image than text.

7 CONCLUSION

The proposed work makes use of AES algorithm to encrypt and decrypt the image and text. It makes use of 128 bit key for encryption which makes AES secure and faster than DES.As the key size is larger, it helps to overcome several attacks such as brute force attack and man in the middle attack. In our proposed system, encryption image doesn't remain the same. The encryption image is chosen in random. So, it is difficult for intruder to differentiate the encrypted image and the original image. So, AES algorithm is most suited for image encryption in real time applications. As a future work, we are planning for a different encryption keys in each round to perform encryption.

References

[1]. William Stallings, "Cryptography and network Security:principles and practice"; Pearson Publication, london, pp. 148-183, 2011.

[2]. Mohammad Amjad, "Security Enhancement of IPV6 Using Advance Encryption Standard and Diffie Hellman", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.182-187, 2017.

[3]. Roshni Padate, Aamna Patel, "Image Encryption and Decryption Using AES Algorithm", International Journal of Electronics and Communication Engineering & Technology (IJECET), Vol.6, Issue.3, pp.23-29, 2015.

[4]. Priya Deshmukh, "An Image Encryption and Decryption Using AES Algorithm", International Journal of Scientific & Engineering Research(IJSER), Vol.7, Issue.2, pp.210-213, 2016.

[5]. M. D. Randeri1, S. D. Degadwala, A. Mahajan, "A Study on Image Encryption Using Key Matrix Generation from Biometric Mixed Fingerprint Image for Two Level Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), Vol.2, Issue.6, pp.486-490, 2017.

[6]. Guang-liang Guo, Quan Qian, Rui Zhang, "Different Implementations of AES Cryptographic Algorithm", In the Proceedings of the 2015 IEEE International Conference on High Performance Computing and Communications (HPCC 2015), New York, USA, pp.1848-1853, 2015.

[7]. Amina Msolli, Abdelhamid Helali, Hassen Maaref, "Image encryption with the AES algorithm in wireless sensor network", In the Proceedings of the 2016 IEEE International Conference on Advanced Technologies for Signal and Image Processing(ATSIP 2016), Monastir, Tunisia, pp.41-45, 2016.

[8]. Siti Zarina Md Naziri, Norina Idris, "The Memory-less Method of Generating Multiplicative Inverse Values for S-box in AES Algorithm", In the Proceedings of the 2008 IEEE International Conference on Electronic Design, Penang, Malaysia, pp.978-982, 2008.

[9]. B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, "Image Encryption Based On AES Key Expansion", In the Proceedings of the 2011 Second International Conference on Emerging Applications of Information Technology, Kolkata, India, pp.217-220, 2011.

[10]. Qi Zhang, Quinding, "Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm", In the Proceedings of the 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, Qinhuangdao, China, pp.1218-1221, 2015.

[11]. P. Thakkar, H.K. Mishra, Z. Shaikh, D. Sharma, "Image Encryption and Decryption System Using AES for Secure Transmission", International Journal of Computer Sciences and Engineering(IJCSE), Vol.5, Issue.5, pp.109-114, 2017.