IMAGE ENCRYPTION USING AES ALGORITHM

[1]Mr.D.Vimal Kumar1, [2]Mr.G.Ajith, [3]Mr.V.Kadhir Anand, [4]Mr.J.Naveen, [5]Mr.R.Thilakesh

[1]AssistantProfessor,[2,3,4,5]Student
Department of Information Technology
Hindusthan Institute of Technology
Coimbatore, Tamilnadu

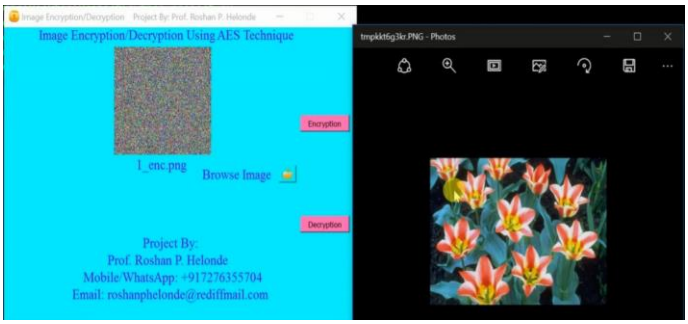
***Abstract*- Image security is important these days as data is increasing a lot. These data can be images, videos, text, audio, etc. so to protect these images from attackers who can destroy the image quality or modify the images, some technologies like AES, DES, RSA, , etc. have been invented. With the generation, data security has also become an essential issue. Considering these issues, the proposed technique ensures confidentiality, integrity, and authentication. Using these techniques, the host can encrypt and decrypt the image and can keep the digital images safe. When AES was chosen 16 years ago, digital technology was completely different from today and the scale of challenges was smaller, so with recent advanced technology and the emergence of new applications such as Big Data applications, in addition to applications running with 64-bit and many other applications have become necessary to design a new current algorithm for current requirements. Advanced Encryption Algorithm (AES) is a symmetric algorithm, which we will further discuss in detail in our research, and in addition to new recommendations for future work, a list of shortcomings and vulnerabilities of the internal structure of the AES algorithm will be diagnosed.**

***keywords*- AES Algorithm, Image Encryption, Image Decyrption, Symmetric Cipher.**

1.INTRODUCTION

The Internet communication plays an important role in transferring a large amount of data to many users every day. Over the years, with the increase in data security, it becomes a problem that data is sent through insecure channels that are exposed to manipulation or attack by malicious users. Various security technologies have been put in place to ensure that data or messages reach only those who are authorized to receive them. Cryptography has been one of the main techniques deployed to secure data through the processes of encryption and decryption. Encryption involves encoding information to secure data from attackers so that they cannot easily access it. This process involves turning "images" into invisible "cipher images" using keys, substitutions, and permutations. In the decryption process, we intend to convert the encrypted image back to the original plain image without missing any pixel from the original image. Carrying out both processes involves the use of mathematical calculations and certain algorithms. The main concern of cryptography is to provide confidentiality, integrity, non-repudiation, and authentication through encryption and decryption algorithms. There are various cryptographic techniques symmetric, asymmetric, and hashing. In this article, we will discuss the AES algorithm which is symmetric cryptography technique.

AES is a data encryption algorithm introduced by the US National Institute of Standards and Technology (NIST) in 2001. The AES algorithm, also known as the Rijndael algorithm, is a symmetric block cipher algorithm that uses 128,192 or 256 bits. Keys to transform a 128-bit message block into 128-bit ciphertext. This method makes it strong, secure, and exponentially stronger than DES, which uses a 56-bit key. The AES algorithm uses a substitution permutation or SP network with several rounds to generate the ciphertext. The length of the key used will determine the number of rounds. The number of rounds shown in Figure 2, 10, applies to the case where the encryption key is 128 bits long. The number of cycles is 12 when the key is 192 bits, and 14 when the key is 256. Before any cycle-based encryption processing can begin, they converted the digital images into a binary matrix to process it through the AES encryption algorithm. It is divided into 4*4 matrix for each unit of 8 bits to form the plain text of the algorithm. The input state field is XORed with the first four bytes of the key schedule The same thing happens during decryption - except now we XOR the state field of the ciphertext with the last four words of the key schedule.



In January, 1997 NIST began its effort to develop the AES, a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES. The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.

which empowers application programming for Android frameworks, is an application in itially given by Google and same time, the speed esteem is determined by

2 .AES ENCRYPTION

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

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.

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.

	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

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

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

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

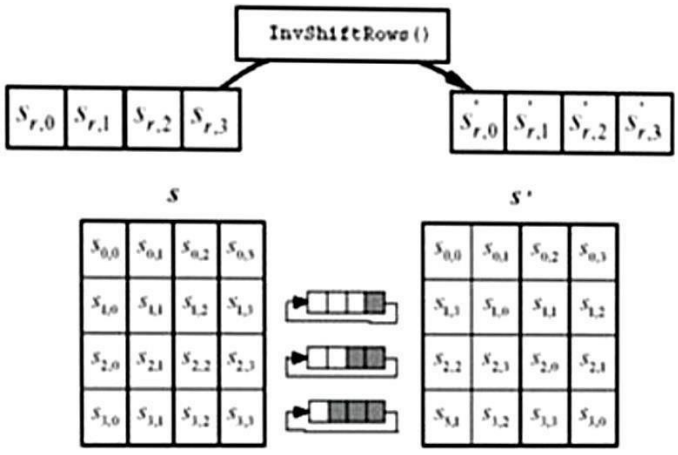
$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

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

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).

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

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.



AndroidApplication

A set of instructions or program required to make hardware platform suitablefor desired task is known as software. Software can also be defined as the utility programs that are required to drive hardware of computer. Operating system-Microsoft Windows 7 SP 1 or above Microsoft Visual Studio 2010 MinGW and Visual C++ compilers (for Windows) Supporting Webcam Drivers

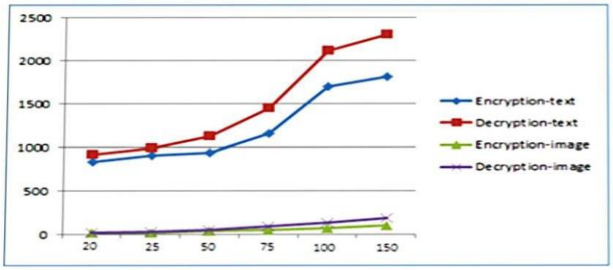


Fig 15. Comparison – Text & Image

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

Figure4: Controlscreen

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-imageand decryption process is enhanced by providing the cipher-image as input, produced the plain-image. Both encryption and decryption utilize the same key.
The time complexity of encryption and decryption for text has been calculatedusing AES algorithm and the following results are obtained.
The time complexity of encryption and decryption for image has been calculated using AES algorithm and the following results are obtained.
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.

Figure 5: Bluetooth connection (a) no action, (b) the scan buttonwaspressed,(c)theconnectbuttonwaspressedand the connected, (d) disconnect button was pressed

Encryption is the process of transforming the original data which called plaintext in to encrypted data called ciphertext. Different techniques are used to fulfill the data own features of each data type. Many encryption algorithms used to protect and ciphered text data such as classical cipher system. Digital images used in many communication applications, therefore the protection the content of these images become very important. Image encryption is a technique which coding the original image (plain image) to another un-understanding image (cipher image). This technique must be providing the decoding the cipher image to plainimage without losing data or image properties . Divers set of applicationsubiquitous depending on digital image encryption and used diver's algorithms to protect the content and information of original images fromunauthorized users. There are different types of encryption algorithms according to plaintext message; some used for text data and not besuitable for other multimedia data such as digital image. Others types used for images and not suitable with text data. Due to image powerful attribute such as vast data capacity, the great redundancy and great correlation among pixels of image.

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]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.
[2]J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer- Verlag, pp. 288-296.
[3]J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.
[4]―Specification for the Advanced Encryption Standard (AES),‖ Federal Information Processing Standards Publication 197, Nov. 2001
[5]A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997, p.81-83.
[6]C.-P. Su, T.-F. Lin, C.-T. Huang, and C.-W. Wu, ―A high- throughput low-cost AES processor,‖ IEEE Commun.Mag., vol. 41, no. 12, pp.86–91, Dec. 2003.
[7]C.-P. Su, C.-L. Horng, C.-T. Huang, and C.-W. Wu, ―A configurable AES processor for enhanced security,‖ in Proc. ASP-DAC, Shanghai, China, Jan. 2005, pp. 361–366.
[8]Rachh, R.R.; Anami, B.S.; Ananda Mohan, P.V. ―Efficient implementations of S-box and inverse S-box for AES algorithm,‖ in TENCON 2009 - 2009 IEEE Region 10 Conference , Nov. 2009, pp. 1–6.
[9]Kaur, Swinder; Vig, Renu , ‖ Efficient Implementation of AES Algorithm in FPGA Device‖ in Conference on..
Grace, S. Kharim, and P. Sivasakthi, "Wireless sensor basedcontrolsysteminagriculturefield,"in2015.